digit Fast Track

to WIRELESS TECHNOLOGIES

- Wireless carrier waves
- Wireless broadcasting
- Cellular telephony
- Bluetooth
- Wi-Fi
- Short range point-to-point communication
- Special applications

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

Fast Track
to

Wireless Technologies

By Team Digit

Credits

The People Behind This Book

EDITORIAL

Editor-in-chief	**Edward Henning**
Editor	**Robert Sovereign-Smith**
Head-Copy Desk	**Nash David**
Writers	**Mohamed Rameez, S Venkatesh** **Siddarth Raman, Liza Ann Easo**

DESIGN AND LAYOUT

Layout Design	**MV Sajeev**
Cover Design	**Kabir Malkani**

Published by 9.9 Interactive

September 2009

Free with Digit. Not to be sold separately. If you have paid separately for this book, please email the editor at **editor@thinkdigit.com** along with details of location of purchase, for appropriate action.

CONTENTS

Introduction

The modern office or home, as far as electrical/electronic appliances are concerned, differs primarily from one ten years ago by the fact that wires have almost disappeared for all practical purposes. Gone is the age of desks cluttered with tangled wires. Today, except for power transmission wires, all wires can be done away with. The internet is wireless, phones are wireless, computer peripherals are wireless. The last frontier, wireless power transfer, is soon about to be breached. The time seems ripe for us to delve into the world of wireless technologies, and the first logical question in this direction seems to be to ask the exact definition of wireless.

1.1 What is wireless?

Put simply – a wireless technology is any technology in which wires have been eliminated in areas where wires were required before. Almost all wireless applications have been in the field of communication (more specifically, in transferring signals and not just communication between humans). Examples range from radio and TV broadcasting to mobile phones, Bluetooth and wireless LAN.

While almost all developments in this direction have been made possible using electromagnetic waves (explained in detail later), some very specific applications have also been developed using ultrasonic (high frequency sound) and infrasonic (low frequency sound) waves.

Before we go into how exactly wireless communication takes place, let us take a brief look at its history.

1.2 History of wireless technologies.

Though the scientific world had been aware of both electricity and magnetism separately for a long time, the connection between the two had not been noticed until the 19th century. Reports in the early 19th century about the connection were largely unnoticed by the scientific community. In 1820, Hans Christian Oersted accidentally discovered that a current carrying wire caused a magnetic needle in a compass to deflect, and became the first to record evidence of the relationship between electricity and magnetism. Soon various theories of electromagnetism, notable ones being from Andre Marie Ampere, etc., were in circulation.

Yet the existence of electromagnetic waves was not even imagined until the 1850s, when Maxwell published his theories of electromagnetism. In a paper named "A dynamical theory of the electromagnetic field", Maxwell published his views regarding the existence of electromagnetic waves. He also summarised all that was known about electromagnetism at that time into the four famous Maxwell equations. Much of the groundwork to his beliefs had been laid by Michael Faraday, who established concepts such as electromagnetic induction, and theorised that electric and magnetic fields extend beyond conductors into the space around them.

In the 1870s and the 1880s, a volley of patents were filed in the United States for devices that could transmit and receive electromagnetic waves. While many of these took huge leaps of imagination, some were quite close to the modern idea of radio. Notable among these attempts, were some by the famed inventor Thomas Alva Edison.

The first major milestone towards wireless transmissions was achieved between 1886 and 1888 by Heinrich Rudolf Hertz, after whom the SI unit of frequency is today named. Hertz demonstrated the transmission and reception of radio signals and was the first person to do so. He also discovered that Maxwell's equations could be reformulated to form a differential equation, from which could be derived the wave equation.

Yet the true birth of modern wireless can be seen in Nikola Tesla's famous article "the true wireless". He soon demonstrated the transmission and reception of radio waves, and then gave a lecture on the principles of wireless

Nikola Tesla, Inventor and Genius.

communication.

This era also witnessed various simultaneous developments in this area. The Indian physicist Jagdish Chandra Bose famously used electromagnetic waves to detonate a cannon and ring a bell at a distance (in 1894), yet showed no interest in patenting it. The first meaningful communication through wireless was demonstrated by Oliver Lodge who in 1894 devised a way to transmit Morse code through radio waves. Other notable contributors in the field include the Russian inventor Alexander Popov and the New Zealander Earnest Rutherford.

Guglielmo Marconi, the father of the modern day radio

However the lion's share of the credit for modern wireless goes to Guglielmo Marconi, who besides being the British patent owner for the first viable radio telecommunications system, is also responsible for commercially developing and deploying the technology. He opened a radio factory in England, employing fifty men.

Jagdish Chandra Bose used electromagnetic waves to detonate a cannon from a distance

In 1901, Marconi conducted the first experimental transatlantic radio communication transmissions. By 1907, this had been commercialised, leading to the first transatlantic radio communication link, between Newfoundland and Clifden, Ireland. Marconi's company, British Marconi, and its American subsidiary, American Marconi, soon started commercially producing ship to shore wireless communication systems and went on to monopolise this sector.

The first steps towards wireless telephony were taken by the German company Telefunken. Founded as a joint venture of the Siemens & Halke company and the General Electric company of Germany, the company created the only semi-permanent wireless link between Europe and North America.

The next significant step in the development of wireless communication technologies came with the invention of the amplitude modulated (AM) radio. This allowed radio transmission by various stations at the same time, using different frequencies, as opposed to the then popular spark gap technology, which covered the whole allotted spectrum. This was achieved by Reginald Fessenden, who also managed to transmit violin music and Gospel readings over the air, to the delight of many ships at sea.

In 1909, the Nobel Prize in Physics was awarded to Guglielmo Marconi for his contributions to radio telegraphy technologies.

1909 also saw the development of radio broadcasting as we know it, with Charles David Harrolds, a professor of electronics from San Jose, setting up a radio station that continuously transmitted music and voice. Harrolds, the son of a farmer, set up the definitions for the terms broadcasting and narrowcasting (transmissions meant for a single recipient). Today, his station has grown into the KCBS San Jose station.

With the sinking of the Titanic in 1914, regulations were implemented that made it mandatory for all ships to have ship to shore radios manned 24 hours. This gave a huge boost to the then fledgling radio industry and propelled the world into a new era of radio telegraphy, and eventually radio telephony.

In 1916, the first radio station to broadcast daily was established by Harold Powers. With his company American Radio and Research Company (AMRAD) the station, call-signed 1XE, became the first to broadcast dance programs, university lectures, news, weather and even bedtime stories. The year 1920 witnessed the birth of the first broadcasting station for entertainment based in Argentina. Significant credit for the popularisation of audio radio must be given to the invention of the radio audio detector that saw the replacement of radio telegraphy.

The sinking of the Titanic was a blessing in disguise for the wireless industry

In the 1920s, with the invention of the vacuum tube, the till then popular crystal set, based on spark gap technology, became obsolete. These radios, however, still have a huge fan

Digitisation

This is the process of converting analogue signals to digital signals.

base among niche group of hobbyists, notably the Boy Scouts of America. Radio technology continued to improve through the 1920s into the 1930s with the improvement of vacuum tube, the invention of the early ancestors of diodes, etc. Some of the major contributors to these achievements was Westinghouse laboratories, based in the USA and, as always, Marconi.

The next great leap in the field of radio came in 1933 with the development of FM. This revolutionary technology insulated the signal from external electronic interference and allowed the transmission of crystal clear audio and other signals across radio waves. However its technological features limited its usage to short range (a city wide, for example) applications.

With the end of World War 2, radio stations and devices spread across Europe and the rest of the world. Soon, radio became a commonplace device. The 1950s witnessed the rapid miniaturisation of radio receivers thanks to the discovery of transistors and diodes. Over the next 20 years, transistors replaced vacuum tubes in all applications except the most specialised.

The 1960s witnessed a new revolution in wireless communications with the advent of communication satellites. With the launch of Telstar – the first communications only satellite, it became possible to transmit across the world, beyond the line of sight. Communication satellites stay in geostationary orbit .

The late 1960s also witnessed the digitisation of radios, mainly in long distance telephone networks. The 1970s saw the advent of radio and satellite navigation systems, originating from attempts by the US navy to precisely navigate their ships. In 1987, the GPS system of satellites was launched.

The 1990s witnessed the birth of various technologies merging computers and other devices such as mobile phones, PDAs and wireless technologies. Wireless LAN, Bluetooth, etc., are the offspring of this revolution.

Geostationary orbit

An orbit where one revolution by the satellite around the Earth is 24 hours, so that it remains directly above one point on the Earth at all times.

It is interesting to note that a form of radiotelegraphy survives to this day. With a high level of automation in encryption and decryption, Telex is a communication medium of choice for businesses such as the banking industry. It is capable of transmitting information and directly printing it.

1.3 Commercial wireless technologies and examples.

Here is a list of commercial wireless technologies available today.

AM radio

Amplitude modulated radio used for long range audio broadcasting. For example, Akashavani.

FM radio

Frequency modulated radio, provides better quality of sound for short range broadcasting. For example, Radio City.

Short wave radio

Used for communications, handheld radios and walkie talkies. For example, radio handsets used by law enforcement agencies.

TV broadcasting

Digitally modulated signals carrying live audio and video for television audience. For example, Tata Sky.

Satellite communications

Satellites in geostationary orbits are used to capture and rebroadcast signals for intercontinental communications. For example, the INSAT series.

GSM

Global system for mobile communications is a cellular telephony technology based on time division and frequency division multiplexing. Operates at 900, 1,800 and 2,700 MHz. For example, Airtel, Idea, etc.

CDMA

This is a cellular telephony technology based on code division multiplexing. For example, Tata Indicom and Reliance Communications.

Infrared

TV remote controls use this as a means of communication.

Cordless telephones

Use radio waves to avoid the wire connecting the handset and the base unit.

GPS

Satellite-based positioning service that uses radio waves.

Wireless peripherals

Use radio waves instead of wires to connect to the PC. For example, wireless keyboard and mice.

Bluetooth

5-GHz short range wireless technology that allows several types of equipped electronic devices to interconnect.

Wi-Fi

Also known as IEEE 802.11a, b, g and n, this allows wireless local area networks to be set up. It also allows local wireless internet connections called hotspots.

RFID

Radio frequency identification devices, in which objects/humans/animals wear small radio tagged devices that allow them to be located. For example, radio collars for dogs.

Wireless carrier waves

2.1 Basic principles and the physics involved

All electronic communication, may it be between humans or machines, wired or wireless, takes place through signals. A signal is a measurable physical quantity, the value of which varies with time in a meaningful manner. The simplest example of this can be found in a microphone, which converts sound (sound is really very small variations in air pressure) using a sensor to a varying electric voltage. Other properties of the signal are maintained. A larger pressure variation leads to a higher voltage change and a faster variation leads to a higher frequency signal. For further understanding of these concepts, let us understand the various properties associated with a signal.

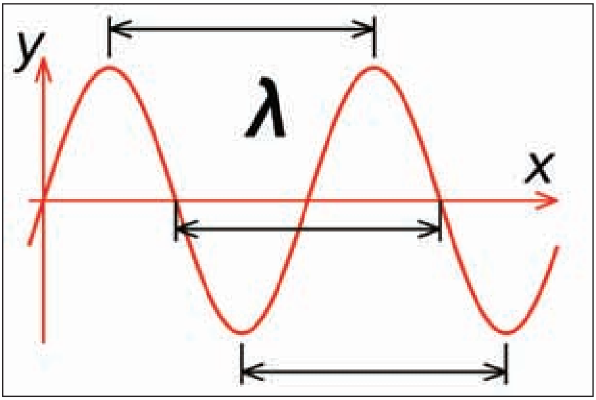
Amplitude

The amplitude of a signal is the maximum magnitude (size) of the varying parameter. In case of an electronic signal, the maximum voltage is the amplitude. In the case of an electromagnetic wave, the varying quantity is an electric field or a magnetic field.

Frequency

The frequency of a signal is the number of times the signal varies in a second. The unit of frequency is hertz (Hz), named after the famous physicist of the same name. If the voltage varies once in a second (one variation is considered to be till the voltage returns to the previous value. For example, if it goes from 0 to 5, and then back to -5 and back to 0. the frequency is considered to be 1 Hz. A thousand hertz is called a kilohertz (kHz), a million Hertz a megahertz (MHz), and so on.

It was the discovery that the speed of radio waves and light is the same that led to the conclusion that light is an electromagnetic wave



The wavelength is denoted by the Greek symbol lambda

Wavelength

This is the length of a single wave in space as the electromagnetic wave propagates. Mathematically, it is the speed of the electromagnetic wave divided by its frequency.

Speed of the electromagnetic wave

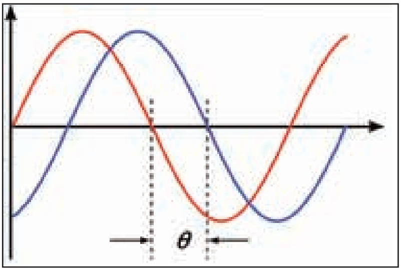
Irrespective of frequency, amplitude and phase, the speed of electromagnetic waves is about 300 million metres per second. This is usually known as the speed of light, light being electromagnetic radiation of much shorter wavelength than radio. It was the discovery that the speed of radio waves and light were the same that led to the conclusion that light is an electromagnetic wave. Visible light, in fact, is an electromagnetic wave in a narrow range of frequencies around about a million gigahertz (10^{15} hertz). Different colours correspond to different frequencies, with red being the lowest and violet the highest. The frequency immediately below the visible range is called infrared and the frequency immediately above is called ultraviolet.

Time period

The time period of a signal is the time taken for one complete variation of the parameter. Mathematically, it is the inverse of frequency and is measured in seconds, milliseconds and microseconds.

Phase

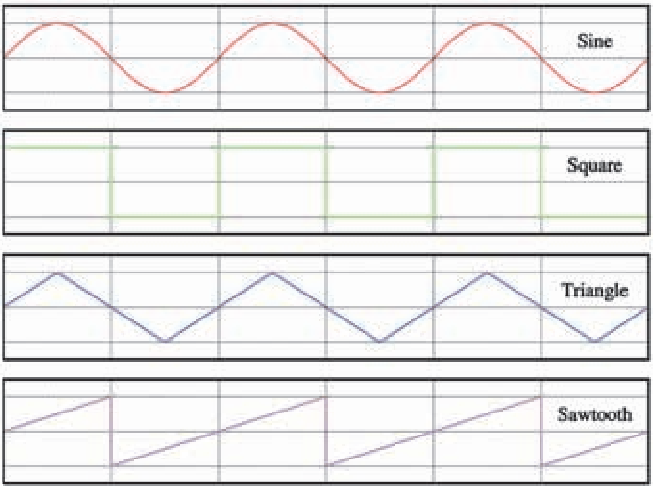
Phase refers to the relative positioning of a signal with respect to another. Two identical signals, one having 5 V at a given moment while the other has 0 V are said to differ in phase – they are not "in step" one might say.



Two waves differing only in phase. Sometimes, phase is expressed in terms of angles, with a full time period being 360 degrees.

Other properties of a signal include the type, shape, etc. If the signal varies from one value to another by going through all values possible in between, it is said to be analogue. If it takes certain discrete values and no values in between (sudden changes) it is said to be digital.

How these signals are formed to carry meaningful information forms an important part of communication theory known as modulation.

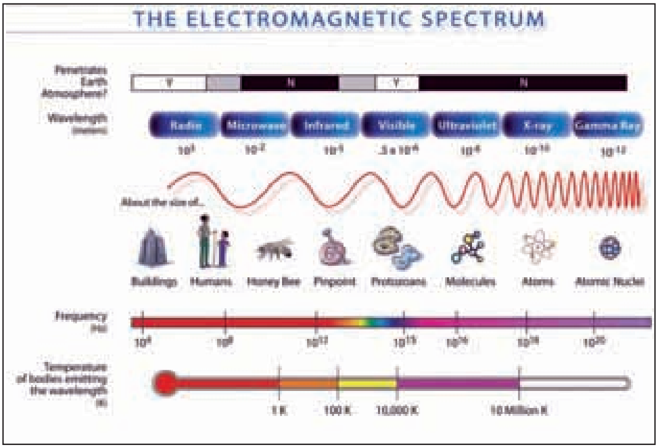


Various signal waveforms. The picture displays how the parameter varies with time.

In the case of a wireless signal, the property that varies (such as voltage in a wired signal) is the electric field. Electric fields do not require a material medium to exist or vary in. According to Maxwell's equations, an alternating (varying) electric field gives rise to a similarly varying magnetic field, and hence such a signal is called an electromagnetic wave. Such waves travel far and wide in space be it vacuum, or occupied with matter. The varying electric field gives rise to a varying magnetic field, which in turn, gives rise to an electric field, and so on. The basic

Band name	Abbr	Frequency and wavelength in air	Uses
Extremely low frequency	ELF	3-30 Hz 1,00,000 km - 10,000 km	Communication with submarines
Super low frequency	SLF	30-300 Hz 10,000 km - 1,000 km	Communication with submarines
Ultra low frequency	ULF	300-3000 Hz 1,000 km - 100 km	Communication within mines
Very Low frequency	VLF	3-30 kHz 100 km - 10 km	Submarine communication, avalanche beacons, wireless heart rate monitors, geophysics
Low frequency	LF	30-300 kHz 10 km - 1 km	Navigation, time signals, AM longwave, broadcasting, RFID
Medium frequency	MF	300-3000 kHz 1 km - 100 m	AM (Medium-wave) broadcasts
High frequency	HF	3-30 MHz 100 m - 10 m	Shortwave broadcasts, amateur radio and over-the-horizon aviation communications, RFID
Very High frequency	VHF	30-300 MHz 10 m - 1 m	FM, television broadcasts and line-of-sight ground-to-aircraft and aircraft-to-aircraft communications. Land Mobile and Maritime Mobile communications
Ultra High frequency	UHF	300-3000 MHz 1 m - 100 mm	television broadcasts, microwave ovens, mobile phones, wireless LAN, Bluetooth, GPS and Two-Way Radios such as Land Mobile, FRS and GMRS Radios
Super High frequency	SHF	3-30 GHz 100 mm - 10 mm	microwave devices, wireless LAN, most modern Radars

The various frequencies and their usage.



The electromagnetic spectrum. Wireless communication applications usually use frequencies lower than (wavelengths longer than) the visual spectrum.

principle is that a current carrying conductor sets up a magnetic field around it that is proportional to the current.

2.2 Frequency spectrum and its use

Electromagnetic waves are almost single-handedly responsible for all wireless technology applications today. Whether it be short range or long range, over the earth's surface or through satellites, carrying voice, images or text, all wireless information ranging from radio communication to wireless LAN are carried by electromagnetic waves. The amplitude, frequency, and the type of the signal will vary according to applications. But the fundamental concept remains the time varying electric and magnetic fields.

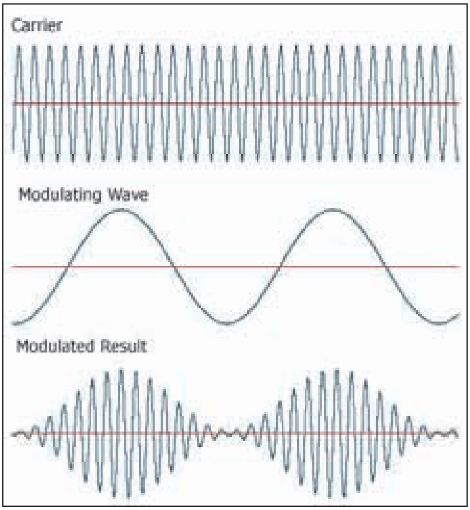
The frequencies used for communication purposes are usually low. This is due to the fact that higher frequencies are generally harmful for human beings, among other factors.

2.3 Modulation

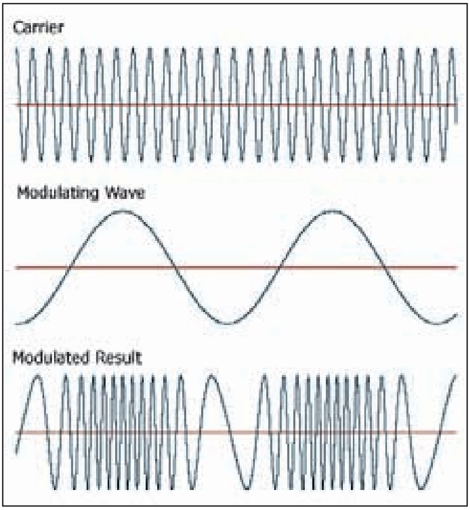
Modulation is the process of shaping of a carrier wave to convey a signal. A digital message can be represented by an analogue wave by a process known as keying. There are multiple methods of keying, including phase-shift keying, frequency shift keying and amplitude shift keying. Bluetooth, which is used by the modern world, uses phase shift keying.

Transmission at a lower frequency results in large losses of energy. Therefore, many signals are transformed into a higher frequency in order to transmit. The signal is superimposed on a higher frequency wave known as the carrier wave before transmission.

The simplest type of modulation technique for digital signals is continuous wave modulation. When the radio operator presses the key the waves will be transmitted and when he leaves the key it stops. This is the basis of Morse code.



An amplitude modulated signal



A frequency modulated signal

There are several techniques to combine the signal and carrier wave. One such technique is amplitude modulation where the amplitude of the carrier wave is varied according to the signal. On the other hand, the frequency of the wave is varied according to the signal in the case of frequency modulation (FM).

2.4 The transmitter and receiver

A transmitter is an electronic device, which, with the help of an antenna, sends an electromagnetic signal such as a radio wave, either to a receiver or a device that will retransmit the signal to a receiver.

A basic transmitter consists of a power supply, an oscillator, an amplifier and a modulator. There are various types of transmitters depending on the varied number of applications. In many parts of the world, the use of a transmitter is controlled by law as it can interfere with waves used for other purposes such as aircraft navigation, and hence endanger lives.

The receiver is an electronic device that receives the transmitted wave from the transmitter. A current is induced in the receiver's antenna by the incoming wave and this regenerates the original signal. The signal is then amplified to drive a reproducing device such as a loudspeaker, tape recorder, earphone or video monitor. The mechanism of reception is in the electromagnetic waves inducing voltages on the metallic antenna which are amplified. Selection is the process of selecting one frequency range from the signal. The better the receiver is at differentiating between the desired and undesired frequencies, the better the selectivity rating. The sensitivity of a receiver is the ability to detect modulated waves from noise. The receiver must have some mechanism to demodulate the signal that was initially modulated at the transmitter. Therefore, it must separate the high frequency carrier wave from the information that was sent.

Probably the simplest of all methods of demodulation is the demodulation of an amplitude modulated carrier wave. It usually consists of a single diode and filter. Other demodulation techniques include:

- DSB and SSB demodulation
- BFM demodulation

Workshop: The simplest sine wave generator.

Now that you know all about electromagnetic waves, sinusoidal waves and how wireless communication works, it is time for you to make your own sine wave generator.

Components required

- An NPN transistor. This is one of the basic building blocks in modern electronics.
- Capacitors. As standard charge storage devices, capacitors are available just as easily as transistors. You will need two 30 microfarad capacitors and a 10 to 100 microfarad variable capacitor box for this project.
- Two 10 ohm resistors. One 1 ohm resistor.
- Connecting wire.

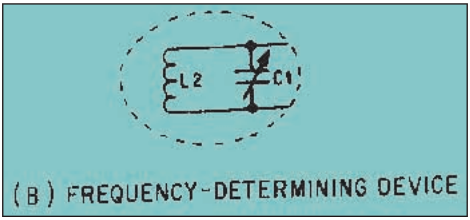
Principle

A sine wave generator is the fundamental component of most transmitter devices. The circuit, known as an oscillator, gives a sinusoidally varying output of a specified frequency and amplitude that can be modified by other circuits to carry meaningful information.

A sine wave generator, otherwise known as an oscillator, consists of three subcomponents. These are:

1. The frequency determining device: this is the device in which when a charge is induced, the charge oscillates back and forth, through simple harmonic motions, and creates a sine wave. However, this circuit alone is not enough as the energy loss inherent to electric circuits will ensure that this oscillating signal will soon die down.

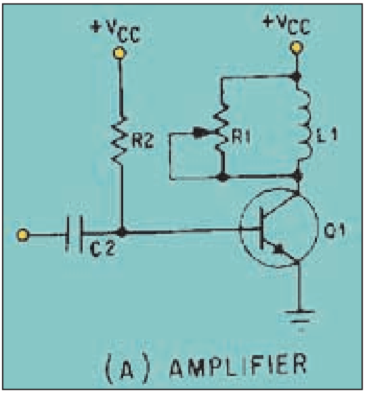
Such a circuit is usually realised in practice by connecting a capacitor and an inductor together. The charge oscillates back and forth, while the energy keeps getting converted back and forth



between the magnetic field of the inductor and the electric field of the capacitor.

2. The amplifier: as mentioned, charge oscillations in an inductor and capacitor alone would soon die down due to energy loss. Hence a device is required to keep amplifying the signal in order to cancel out the loss so that a constant sinusoidal signal may be maintained.

Such a device is usually realised by using a transistor to amplify the signals.

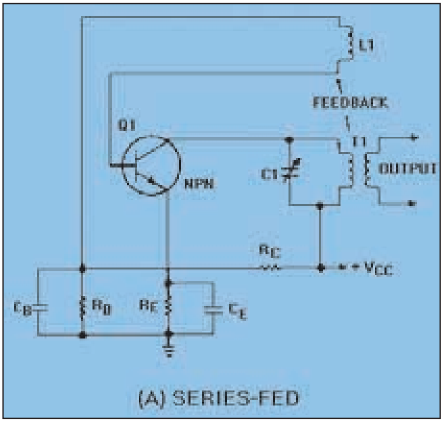


(A) AMPLIFIER

3. The feedback: the signal taken from the inductor–capacitor circuit needs to be fed back into the circuit after amplification. This is usually done through another inductor which realises this using the principle of electromagnetic induction.

Wire up the circuit as shown. Cb and Ce should be 30 microfarads while the variable capacitor box takes the position of C1. Inductors T1 and L1 are to be made by coiling wire around a pencil.

Instructions for wiring the transistor: of the three lines inside



(A) SERIES-FED

the transistor (the round symbol at the centre), the vertical one is the base. Of the remaining two, the one with the arrow mark is the emitter while the other one is the collector. When you are holding the transistor with the flat face upwards and the leads pointing towards you, the leads from the left to right are in the order emitter, base, collector.

To test your creation, take the wires from the output and connect to a headphone or speaker set. If you are using a headphone, one wire should be in contact with the tip of the mini plug while the other is connected to the side. For more stable connections, you may cut off the mini plug and connect to the wires directly.

Switch the circuit on. You should be able to hear a constant pitch hum on the headphone/speaker. Vary the capacitance of the variable capacitance box. Notice that the pitch of the sound changes. This is because the change in capacitance causes a change in the frequency of the generated signal, which in turn causes a change in frequency of the sound, and hence in its pitch.

Alternatively, to test your circuit, you may connect the output to a cathode ray oscilloscope (a device used to form images of waves on a screen). However, we will not explore that option here.

Wireless broadcasting

The term broadcasting was coined by Charles Harrolds, a professor of electronics at San Jose University. The son of a farmer, he drew analogies between the transmission of signals and the sowing of corn. Broadcasting was then a popular term used to describe the sowing of corn far and wide. So, all signal transmissions intended to reach a large number of receivers came to be known as broadcasting. The core difference between wireless broadcasting and other wireless technologies is that broadcasting is essentially one way. There is a fixed transmitter and many fixed receivers, unlike with technologies such as Bluetooth where communication takes place both ways.

3.1 Television broadcasting

Almost undeniably the most popular form of broadcasting today, television broadcasting is the transmission of video signals in the form of a large number of still images per second, associated with simultaneous audio. TV broadcasting today takes place through radio waves and also through local cable networks.

All of today's TV signals are transmitted in the 54 to 890 megahertz frequency band. Up to the year 2000, the majority of TV signals were transmitted using analogue signals, but recent years have witnessed this largely being replaced with digital signals using digital modulation techniques. While

An early model television set

almost all channels today transmit using stereo audio (two channels of audio), some channels have switched over to surround sound transmissions (three or more channels of audio, to give a more realistic perception of sound).

With the origin of the idea in some science fiction works of the 1870s, television, then known as the telephonoscope was deemed inevitable with the rapid development in the ability to generate and transmit images. The earliest ancestor to the television can be seen in the telephonoscope built by Paul Gottlieb Nipkow in 1884. This design used a pendulum with holes in it, swinging in front of selenium plates that were sensitive to light. Producing extremely poor quality images by today's standards (it would appear to be a series of black and white dots of varying size), these images still could not be displayed on screens until the technology became available in 1907.

The true father of modern television is John Logie Baird, a Scottish inventor who improved the device designed by Nipkow to transmit outline images in 1925, and later full images in 1926. He used a scanning device which could scan 30 vertical lines, just about enough to capture a discernible human face. He also pioneered the concept of video recording, modulating the video signals down to the audio frequency range and storing them on small disks available at that time. These disks were, in the early 1990s, converted back into viewable images, using advances in digital signal processing.

The telephonoscope built by Paul Gottlieb Nipkow in 1884 made way for the television as we know it today

Soon methods were devised to convert the electronic video signals into radio waves, and to transmit, receive and display them like audio signals. By the 1960s, television had spread to almost all parts of the globe and by the 1990s almost every country had its own broadcasting stations. Certain other notable developments in television technology were the advent of satellite broadcasting, the birth of digital and later high definition television.

Wireless broadcasting of television signals can be broadly classified into two categories.

Terrestrial broadcasting

The only form of transmission possible before the advent of the satellite Early Bird, in 1965, this form of transmission was limited in range by the curvature of the earth. Ranges were slightly over line of sight (due to some signals bouncing off the ionosphere, a layer of the atmosphere). Prior to the advent of communication satellites, the only way to transmit long distance, beyond visual range signals, was through a continuous system of high altitude aircraft maintained in a loop, a technique devised by Westinghouse radio. Today, terrestrial television is facing extinction due to strong competition from satellite television, a trend that might be reversed due to the recent introduction of high definition television (HDTV, explained later). HDTV can be transmitted only through terrestrial broadcasts due to the bandwidth limitations of satellite television. High definition television contains mush more information in its images, and so requires a much larger bandwidth than standard television. Terrestrial television is received using a standard dipole antenna (the old ones in the shape of a skeleton). e.g. Early Doordarshan

Although terrestrial broadcasting has come nearly to an end, HD transmission may revive it unless satellites become capable of handling the high bandwidth

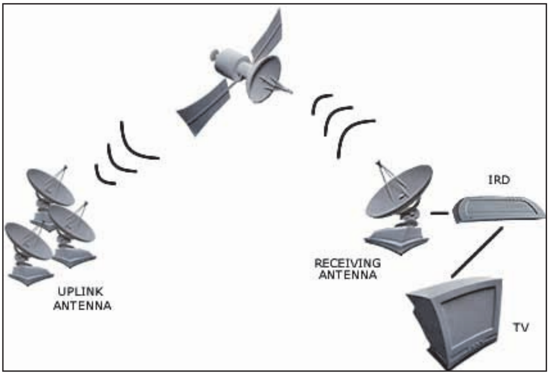
Satellite broadcasting

The predominant form of television broadcasting today, this began with the satellite Early Bird in 1965. Satellite broadcasting quickly gained popularity over terrestrial broadcasting due to the inherent cheapness of the technology. Terrestrial broadcasting to a geographically dispersed target audience was expensive, due to the large number of repeating stations and towers required. The first country to operate a nationwide fully operational satellite television network was the Soviet Union, through the Molniya series of satellites. Satellite broadcasted signals are received using a dish antenna and a set top box. The signals can be encrypted (coded in a way that can be decoded only by select set top boxes), making it possible to exact payment for subscription.

Let us now take a brief look at how satellite broadcasting works. Today, most customers use the direct to home model, where many TV channels are broadcasted by a direct broadcast satellite provider (such as Tata Sky). At the broadcast centre, or the Playout and Uplink location, the various channels are compressed to make the data stream small enough for satellites to handle, encrypted so that non paying receivers cannot receive the signal and transmitted to a satellite in geostationary orbit. A geostationary orbit is one in which the time period for one revolution of a satellite is exactly the same as the rotation of the Earth. Hence the satellite will remain over one point on the earth's surface always, serving as a highly elevated repeating station.

The satellite receives the signals, amplifies them and beams them back onto the earth's surface where dish antennas pick them up and focus them onto the LNB. The LNB is the small box like device found at the centre of dish antennas. Standing for low noise blocker, the function of an LNB is to filter out the noise (non data-carrying signals). The LNB forwards the filtered signal to the set top box which then decrypts the signal using a decryption chip provided by the service provider (a card that can be inserted into a slot on the set top box, in most cases). The signal now decrypted and converted to analogue for playback by a standard TV, is sent to the TV for playback.

The recent rise in popularity of large screens and projectors has rendered many television broadcasting technologies



A schematic diagram of satellite broadcasting.

obsolete. The new era requires much higher resolutions, so that the picture remains sharp on a large screen. Enter HDTV. Broadcasted at far higher resolutions than standard television (the highest being 1920x1080, a resolution supported in Windows only on high end graphics cards), HDTV has already captured a sizeable portion of the market. Many channels today broadcast in HDTV, while many countries are quickly trying to set up HDTV standards.

From being an essential service for news and general awareness, the radio is now popularly regarded as a means of entertainment

As the primary mode of entertainment for the majority of the population, television continues to dominate. With continuous improvements in both image and audio quality, this trend is expected to continue for the foreseeable future.

3.2 Radio broadcasting

Despite the popularity of television and the widespread availability of the internet, broadcast radio tenaciously clings onto a sizeable audience. Some say the attractiveness is in its inherent simplicity and reliability; some attribute it to the fact that entertainment in the audio form dominates the audio industry. Whatever may be the case, any discussion on the topic of wireless broadcasting will remain incomplete without the mention of broadcast radio.

With the exception of internet radio and cable radio, both of which we will not deal with here, all audio transmissions occur wirelessly over radio waves. Radio broadcasting stations of every type, commercial, non-profit, public, private, etc., can be found in all parts of the globe. Some are even run by students on campuses, while some are for emergency utilisation by police, etc.

The majority of radio broadcast stations today can be classified into two: AM and FM.

AM, standing for amplitude modulation (a technique for converting audio signals into transmittable radio waves, explained earlier) is the older and simpler of the two. Although fast being eclipsed by the popularity of FM and internet radio, AM continues to be popular due to its high range (often extending to thousands of kilometres at night). In India, All

An early model transistor radio

India Radio maintains many national and local AM stations. Apart from this advantage, AM radio can be detected and listened to using extremely simple equipment. With a strong enough signal, even a power source is unnecessary. Building an un-powered crystal set radio is a major childhood hobby activity for many hobby groups, and detailed instructions for this are commonly available. However, AM radio is held back by the fact that its signals are extremely sensitive to atmospheric conditions. Storms, solar flares, even wind, often disrupts good quality reception, confining AM to serve as a very utility oriented mode for radio broadcasting.

Frequency Modulation (abbreviated FM), is the undeniable star of today's radio broadcasting community. Crystal clear audio can be transmitted over acceptably long ranges via FM. FM signals are largely unaffected by atmospheric conditions. Requiring relatively lower bandwidth per channel, FM is now mostly transmitted in stereo, making it comparable to personal music players in sound quality.

Invented by Edwin H Armstrong in the 1930s as an answer to the problems inherent with AM, FM remained unpopular till the 1950s. Confined to frequencies between 42 and 50 MHz, FM remained largely a radio enthusiast’s tool and the broadcasts were short, sporadic and experimental. The fact that the reception of FM signals required a different, special receiver also contributed to its lack of popularity. With the end of World War 2, more importance was given to improving the quality of radio transmissions. AM radio, by then suffering from a large amount of interference in the atmosphere, was begging for a replacement. Soon, the currently used frequencies of 88 to 108 MHz were allotted to FM and FM started gaining in popularity. Until the 1970s FM remained merely an alternative to AM, with service providers often transmitting the same programming on both AM and FM simultaneously. This practice was called simulcasting. By the 1980s, with all new radio receiver sets also being equipped with FM capabilities, FM had all but replaced AM in cities. AM however continues to be used, to this day, in rural environments.

Some examples of FM stations in India are Radio Indigo and Radio Mirchi.

The large bandwidth allotted to FM radio has allowed it to be used for other purposes as well. Some broadcasters use this extra capacity for transmitting background music for public places, financial market data for wireless stock tickers, and auxiliary GPS signals.

Aside from AM and FM, a few other technologies for radio broadcasting exist. Chief among them is digital radio, otherwise known as digital audio broadcasting. This technology utilises digital modulation techniques. However it has not gained much popularity and is not expected to do so. A more popular alternative radio technology is satellite radio. Slowly developing, this technology combines digital modulation techniques with satellite based transmission. Allowing for high quality radio, and many allied services, the only drawback of this technology is its relatively high cost, thanks to the requirement of reception apparatus similar to that which is required for satellite TV. In India, the only established satellite radio provider is WorldSpace

The worldspace satellite radio receiver

Satellite radio. This provider boasts of channels in most Indian regional languages, apart from national and international news channels in English and Hindi.

While commercial radio broadcasts were taking over the world, the inherent simplicity of radio transmitting technology and the need for an open non-centralised communication system gave rise to a culture of amateur radio operations. Often transmitted from home built transmitters, this community forms an undeniably important part of the modern radio scene and will be the subject of our next discussion.

In keeping with the entertainment aspect of radio, satellite services such as WorldSpace bring numerous music channels to your room

3.3 Amateur (HAM) radio

Spanning six million people today, the amateur radio community is at the forefront of further developments in wireless communication technology. Using different bands of frequencies and techniques of modulation, amateur radio operators often use home built equipment for their purposes. These operators, more popularly known as hams, enjoy free communications, sometimes extending around the globe among themselves. The origin of the term ham is attributed to many different events, none of which can be supported with certainty.

The history of amateur radio is long and illustrious. Its origins can be found in the origins of radio itself with its pioneers being the various inventors and scientists who contributed to the development of radio. While a large amount of credit goes to Marconi, Edison, etc., credit is also due to lesser known pioneers such as Reginald Fessenden, Amos Dolbear and others.

The radio spectrum was largely unregulated and open to amateur hobbyists until 1912, when the sinking of the RMS Titanic changed everything. The Radio Regulatory act of 1912 in the USA allotted various spectra to various purposes, made ship to shore communication radios mandatory on all ships, and made it necessary to man them 24 hours. This act placed a lot of restrictions on the bandwidths and frequencies available for amateur operators of that time and made roughly 80 per cent of the amateur operators give up their hobby. However, a large number of them continued and utilised the unregulated portion of the spectrum.

By 1917, all amateur radio operations had ceased as a result of a congressional regulation in the United States due to World War 1. This regulation even demanded the dismantling of amateur radio equipment. However, amateur radio operations were allowed to continue after the war and restarted on the 1st October 1919. By the 1920s, hams were competing across the world to build more powerful transmitters and receivers. The development of single side band modulation (a modulation technique used at high frequency that provides low quality audio, albeit at exceptionally high reliability) has been attributed to hams.

By the 1930s, further regulations were placed on hams across Europe and America. However, certain bands were also protected and allotted to them. By the 1940s, hams gained a lot of attention due to their assistance with the war efforts. Father Maximilian Kolbe, a Polish ham operator, was arrested by the Nazis and imprisoned at Auschwitz, where he died a martyr saving another man's life. He was later canonised by the Catholic church and is today the patron saint of amateur radio operators.

During the world war, with almost all the amateur radio operators in the allied countries joining the armed forces, their resources were pooled to create the war emergency radio service. It remained active until 1945. With this service dismantled in 1945, the hams were in possession of a large supply of wartime radio equipment, which would later be converted for amateur use.

Throughout the 1950s, amateur radio gained popularity across the world. With the launch of the first amateur radio satellite (OSCAR) in 1961, amateur radio became practically global. Hams across the world continued to provide essential services during war and peace, disaster and rescue. Some notable contributions were during the Falklands crisis, among others.

Hams have played a vital role in emergency situations since the days of the World War

The 1970s also witnessed further regulation of hams, with hams having to take exams to obtain licences before they were allowed to transmit. This was done first in the US, but other countries quickly followed.

By the 1980s, hams had started integrating computers into their systems. Advanced techniques such as digital signal processing were applied by hams to amateur radio services, pioneering many developments in the world of wireless communication such as phase shift keying (a modulation technique used for digital audio signals).

In India, amateur radio started in the 1920s, and by 1930 there were 16 licensed hams. Hams played a crucial role during the Indian independence movement, as various amateur radio broadcasts were set up illegally against the government. Notable among these is the Azad Hind radio set up by Indian ham Nariman Abarbad Printer. He broadcasted Gandhian protest music and uncensored news, for which he was immediately arrested and his equipment seized. The Congress utilised amateur radio services to coordinate activities with the grass root lever workers during the Quit India movement. Hams also provided valuable communication support for the resistance and the invading Indian National Army under Subhash Chandra Bose.

Post independence, India's first organisation of hams, the Amateur Radio Club of India, was set up in 1948. It was soon converted to the Amateur Radio Society of India and is today the primary amateur radio organisation in India. By 1980, there were 1,600 licensed hams in India. With the waiving of import duty on radio equipment in 1984, the number of hams started rising steadily. Hams continued to play a major role in most emergencies. In the 1991 Gulf War, a lone Indian ham in

An amateur radio operator in India

Kuwait was the only mode of communication between Indian expats in Kuwait and their relatives in India. Hams played a crucial role during the 1993 and 2001 earthquakes. The 2004 Indian Ocean tsunami also created a great amount of ham involvement in India. With the launching of HAMSAT in 2005, India joined a small club of nations to have launched its own amateur radio satellites.

With more than 16,000 licensed hams in India today, amateur radio is an exciting movement to be part of. To become a ham yourself, the easiest way is to join the nearest ham club. For information on your nearest ham club, visit www.hamradioindia.org . You will be required to complete exams in order to obtain a ham licence.

3.4 Other dedicated radio broadcasting networks

Many other types of dedicated radio broadcasting networks are run in the short wave spectrum. Many of these are operated by private companies for specialised applications, such as radio taxis. A service wherein a taxi is available via a phone call, and all the taxis are networked together via radio. Specialised broadcasting services are also run by the police, military and fire department in case of emergencies. In India, both the CRPF and the Territorial Army operate their own radio broadcasting networks. These networks exist as a source of communication in case of the failure of all other systems.

A two way police radio.

Workshop : Tuning your TV and Radio

Tuning your TV and radio might seem one of the most simple things to do. But it has its own intricacies.

All radios today come with an AM-FM-SW selector button. This button might be labelled "mode", and it allows you to switch between these three modes. If you are searching for an AM source press the button until the AM option is highlighted.

Use the up and down keys to flip through the frequencies until you reach the frequency of your preferred station. Some older radios without digital displays (radios that have a knob and a dial with moving arrow to indicate the frequency) usually have two knobs for tuning. One is labelled rough and the other fine. Adjust the knob labelled rough to approximately the frequency you desire (until you start hearing something) and then use the knob labelled fine to tune it to a much clearer signal. The FM radio tuning process is simple.

Some newer radios come with an option known as scan. This button automatically searches for stations. Keep pressing the button repeatedly until your desired station is found.

Tuning your TV involves slightly higher levels of complexity. However, most TVs and set top boxes today come with a built-in auto tune option. All you have to do is turn this on and it will find all the channels within the specified spectrum. Digital satellite TVs and set top boxes also often require you to select the satellite to which you are tuning. Find the specifications from your channel and tune for it. The specifications for a typical satellite TV channel include:

- Frequency
- Satellite
- Polarisation (Horizontal/Vertical): this feature decides what plane the oscillating electric fields of the carrier wave are confined to (Chapter 1).
- Symbol Rate: this is roughly a specification of the bandwidth of the station, as multiple stations might be broadcasted at the same frequency.
- FEC (Forward Error Correction): a technique wherein each piece of data is repeated multiple times, to create more reliability due to redundancy.

All these specifications will be available for the channel you are searching for at its website or any other promotion materials. All you need to do is enter these specifications, and click for search. The set top box/TV should automatically find you the channel you require.

Cellular telephony

4.1 Introduction and history

Mobile phones, otherwise known as cellular phones or cell phones, are possibly the best things since sliced bread. While all mobile phones allow quick communication on the move from a lightweight, low power package, some of the newer features also include high speed internet access, multimedia messages, etc.

Let us take a brief look at how this wonderful technology came into being.

The origin of mobile phones can be found in the early days of the development of radio. Initially, it was just two way radios. While these radios could call each other, they could not call a traditional fixed line phone. These types of radios were bulky, often weighing tens of kilograms and were intended to be used only as car phones. They gained a large customer base amongst truck drivers and other travellers.

A modern cell phone

Soon, attempts were made to overcome the limitations of these designs. In 1945, an experimental system was tested wherein a single base station (similar to a mobile phone tower of today) transmitting a powerful signal covered a whole area. It could operate just one phone at the same time, as concepts such as sharing frequencies were not defined until the 1970s. It was similar to the cordless telephone of today. This technology is now known as 0G (zero generation) and saw no commercial applications.

The inventor of the first practical mobile phone that could be used in a non-vehicle environment

From car phones to GSM, CDMA and WCDMA to even satellite phones, wireless communication has grown significantly over the years is considered to be Martin Cooper, a Motorola researcher. In 1973, he filed a patent for a “radio telephone system”. This kicked off the era of the mobile phone. By 1979, NTT of Japan had a fully operational city-wide cellular network.

The first practical cellphone, the Motorola DynaTac 3000X

The USA’s first approved mobile phone, the Motorola Dynatac, appeared in 1983. By 1984 Bell labs had developed the technology of the cellular phone, the ancestor to the modern cell phone. This technology relied on multiple base stations or cells (towers) each covering a small area. The switching technology required to ensure that a telephone conversation can continue as a cell phone moves from one cell to another was also developed then. By the late 1980s, mobile phones based on this technology, known as 1G (first generation) mobile phones were quite popular in the US, Japan and the Scandinavian countries. The first generation differed from modern mobile phones in that 1G phones were essentially analogue. The voice signals were not encoded, merely modulated to a higher frequency.

The first mobile phone essentially used the same technology as is popular today. The 2G digital standard, was launched in Finland in 1991. This utilised digital signals and was based on the now popular GSM technology. SMS was introduced in 1993 in Finland. Ever since then, mobile phones have not looked back. 2G gave way to 2.5G and now 3G.

Today, the mobile phone technologies used in India can be divided into two - GSM and CDMA.

4.2 GSM

The leading mobile phone standard in use in the world today, GSM is the technology used by providers such as Airtel, Vodafone, Idea and Aircel. The advantages of this system come from the fact that most providers worldwide use this, resulting in easy interoperability of service providers. This allows services

A GSM cellular tower top

such as international roaming to be easily implemented. The fact that the network specifications of the phone are obtained through a SIM (Subscriber Identification Module) card allows users to switch handsets at will, by just moving the SIM to another handset. GSM is the undeniable market leader in mobile phone technologies today, and is expected to remain in this position until 3G takes over.

The origins of GSM date back to the year 1987 when 13 European countries came together in the signing of a memorandum of understanding to develop a common, uniform interoperable cellular telephone standard. The responsibility was soon entrusted to the European Telecommunications Standardization Institute (ETSI) in 1989 which was followed by the publication of the GSM standard in 1990. Further updated versions were published later. One of the primary distinguishing features of GSM was the fact that all features of it were digital. This made it future compatible and capable of later adopting features such as data communication. By 1993, the standard had been updated to support short messaging service (SMS). In 1997, the standard included general packet radio services

(GPRS), a module that would allow the user to access the internet while on the move. This culminated in the 1999 update which led to the inclusion of enhanced data rates for GSM evolution (EDGE) in the GSM standard. EDGE allowed for higher bandwidth internet connectivity.

GSM is a cellular telephone standard. This means that base stations with which the mobile phones communicate form cells. The mobile phone communicates by searching for the closest cell with the highest signal strength. While the phone is on the move, the mobile phone has to switch from one cell to another. This process is called handing over.

GSM has its origins in Europe with nations coming together to unify their wireless communication standards in the early 70s

As a second generation mobile telecommunication standard, the challenge faced by GSM was that it had to allow multiple cell phones to use the same frequency spectrum. It performed this through a technique known as time division multiple access (TDMA). Under this scheme, the conversation of one user for a small finite duration is recorded, encoded and transmitted in a burst that lasts much shorter than the duration of the conversation. Thus, at any given moment of time, only one of the many cell phones within a cell is transmitting at the given frequency. This procedure is known as time division multiplexing. The maximum number of simultaneous calls a cell can handle is given by the length of the finite duration of conversation divided by the length of the burst. This varies depending on factors such as the type of cell and the standard used.

GSM uses a specific set of frequencies. In India, all providers use either the 900 MHz or the 1,800 MHz spectrum. Most European networks operate at 2,100 MHz, while Canadian and American networks utilise the 950 MHz spectrum. Each of these frequencies is known as a band of the GSM spectrum. A phone handset is said to be Quad Band if it can operate at all these frequencies. Similarly, Tri Band if it can operate in three out of the four frequency bands.

In GSM, each connection is identified by a unique SIM card, while each handset is identified by an international mobile equipment identification (IMEI) number. This provides for a moderate amount of security. In later versions of GSM, the signal from the phone to the base unit can be encrypted, after the phone is authenticated (recognised as genuine) by the base unit.

The SIM Card

4.3 CDMA

The other major standard for mobile telephony in use in India, CDMA (Code Division Multiple Access), is the standard used by operators such as Reliance Communications and Tata Teleservices. While not allowing easy interoperability between networks or interchange ability with handsets, some argue that the CDMA standard is still better for India as it allows for much lower power requirements at the base station. The CDMA standard also witnesses very few low coverage problems due to the fact that the range of each cell is very high.

The core concept behind CDMA phones (the standard is more technically known as the IS 95 standard, and is patented by Qualcomm, a US based company), is code division multiplexing. While GSM chooses to divide the transmissions in time from multiple phones in a cell, CDMA transmits all of them at once, encrypts them, breaks them down into coded packets which are transmitted over a wide spectrum of frequencies and reassembled at the base station. The advantages are obvious, whereas GSM cells have a maximum number of phones that can make simultaneous calls (you will presumably often have come across the "network busy" error message on your GSM phone), CDMA phones have no theoretical limits on the number of phones within a cell. Hence, unlike GSM phones, CDMA phones do not have a specific

An interesting story behind CDMA is the battle between Qualcomm and Ericsson over the technology. Ericsson backed out giving way to Qualcomm ownership over CDMA narrow operating band or frequency. In a high population density country such as India, CDMA proves to be cheaper for operators in the long run.

Recent CDMA standards have started incorporating some of the advantages of GSM. One step in this direction was the introduction of the removable user identification module (RUIM), the CDMA equivalent of the SIM card. Not only does this allow the user to switch handsets easily; but, in some countries such as the US, it also allows the user to use CDMA phones on a GSM network with which the provider has a roaming agreement.

4.4 General packet radio services (GPRS)

Put simply, it is a modification to the GSM standard that allows one to access the internet whilst on the move. It allows for speeds as high as 114 kbps. The introduction of GPRS to the GSM standard allowed users to use the following applications:

Multimedia messaging service (MMS): an extension to the SMS service that allows transfer of pictures, video and audio as messages.

Push to talk (PTT): a feature that allows the user to use the phone like a two way radio, pressing a button to be immediately connected to a closed group of people.

WAP: abbreviation for wireless application protocol, this feature allows applications on the mobile phone to connect to the internet.

Email: runs on WAP.

With the introduction of GPRS, GSM is considered to have become a 2.5G standard.

Web browsing on GPRS

In 1999, the GSM standard was modified to include EDGE (enhanced data rates for GSM evolution). By 2003, providers had started implementing EDGE. EDGE is a technology backward compatible to GPRS. It allows for transfer rates as high as 1 Mbps.

With these improvements on GSM and equivalent ones in CDMA, mobile technology continues to improve. Today, both GSM and CDMA are threatened by 3G services such as UMTS. Steps have been taken towards even the next generation, namely 4G. Let us take a look at these.

4.5 Emerging technologies

Most of the emerging technologies in the field of cellular telephony can be classified under 3G. Standing for third generation, this is the name given to a class of technologies that involve GSM with EDGE, UMTS (a new 3G mobile standard) and CDMA2000, an advanced version of the IS 95 CDMA standard. 3G also includes WiMax (Long range wireless LAN) and DECT (Digitally Enhanced Cordless Telephony, the technology used in modern cordless phones.) The unifying features of these technologies are high data rates, high security, etc.

UMTS

A 3G technology otherwise known as W-CDMA (Wideband Code Division Multiple Access), UMTS combines the features of CDMA and GSM to create a completely new technology. While UMTS phones require completely new networks (completely new cell transmitters) the technology is quite compatible with GSM, and UMTS phones can work on both GSM and CDMA networks with reduced functionality. In India, UMTS services are provided only by BSNL mobile, and only in selected cities. UMTS allows a maximum theoretical data rate of about 21 megabits per second, though deployed capacities currently support only up to seven megabits per second.

UMTS runs on the frequencies of 2,100 and 1,700 MHz. Canada uses 1,900 MHz while other parts of the world can be found to use 850 MHz.

With promotional campaigns focussing on high bandwidth applications such as videoconferencing and mobile TV, UMTS

A 3G mobile handset

is expected to gain a significant amount of market share in the near future.

4G

Seen as the next step in mobile telephony, 4G is a futuristic improvement being planned on 3G UMTS networks. 4G aims to develop a standard for deploying networks that provide integrated data services that include high speed internet access, videoconferencing, mobile TV and of course telephony. The aims of 4G are to have data rates as high as one Gbps when stationary (100 Mbps while moving). The standard also aims at surpassing the theoretical number of users per cell defined on conventional GSM and CDMA networks. Other objectives include seamless interoperability with all other networks, backward compatibility with reduced functionality on regular 2G and 3G networks, etc.

Satellite phones

Designed to provide connectivity to regions of the world that are hard to connect through regular cellular networks, satellite phones work on the same basic principles involved in cellular phones. The satellite phones of today are larger than the average cell phone and appear similar to an early 1990s or late 1980s model mobile phone.

In a satellite phone, instead of a tower or an elevated platform, the base station is placed on a satellite. The satellite might either be in geostationary orbit or lower Earth orbit. While the satellites in geostationary orbit provide extremely reliable communications, the very high altitudes of these satellites ensure that there is a noticeable delay in conversations. Also, the signals are much harder to pick up indoors.

The other alternative, lower Earth orbit satellites, manages to avoid these shortcomings. However, as the satellites travel extremely fast over the Earth's surface, a larger network of satellites is required to maintain constant connectivity.

Thuraya and Inmarsat satellite phones operate on geostationary orbit satellites. Thuraya provides complete connectivity to the Middle East, Asia and North Africa. Companies such as Iridium provide full global coverage using lower Earth-orbit satellites.

While an attractive alternative to mobile phones in rural areas, satellite phones continue to be unpopular due to their prohibitive costs. The cheapest handset with connectivity would today cost upwards of Rs. 40,000, plus a "large" monthly bill.

A Thuraya satellite phone

Bluetooth

5.1 Introduction and history

Today, there is a lot of choice when it comes to communication. From utilising direct speech, to using the telephone, mobile networks, the internet via chat or VoIP, the choices are endless. Mobiles are extremely common today, with different technologies allowing users to connect with each other across various frequencies. If you have a mobile phone, or have friends who own one, you would know what Bluetooth is. In simple layman's terms, Bluetooth is a way of interfacing enabled devices in the vicinity. Today, Bluetooth has become an efficient medium for transferring data, playing games and interfacing devices wirelessly.

The 1990s were a good time for the development of the wireless industry, with various standards and protocols emerging and people improving connectivity. Bluetooth emerged as an idea in order to create a wireless local area network, which later came to be defined under the term "Personal Area Network". Bluetooth was first developed in Scandinavia by Ericsson Mobile Communications in 1994. The people with the concept were Dr. Sven Mattisson and Dr. Jaap Haartsen.

The larger idea behind Bluetooth was the MC link which was a short range link between the phone and a communication device

Ericsson initiated a study to investigate an alternative to cables. How would one connect cellular phones with headsets and other devices without cables or wires? The answer: a low-power, low-cost radio interface. The idea as Ericsson put it was not just to connect people across the world, but also to connect users across the room. A simple attempt to simplify communication between electronic devices fostered and pioneered an entire enterprise. Today, Bluetooth is enabled in several devices. Telephones, mobile phones, computers, video game consoles, digital cameras – all can now be interfaced and linked with Bluetooth. The idea of Bluetooth was also a subset of a larger idea they were working under – the MC Link which was a short-range communication link between the phone and the communications device.

The technology was new, moreover it was cheap since it was tapping into a low-frequency radio band that required no licensing, meaning that everyone in the world could use it. However, what they realised was that if they did want Bluetooth to be a universal communication medium that every person could use to interface with surrounding electronic devices, other manufacturers of equipment would have to adhere to similar standards. Hence, in 1997, Ericsson decided to give away its technology for free. Bluetooth was no longer its property.

The name has an interesting origin, as does the logo. The technology, since it was pioneered in Scandinavia, was named after King Harald Bluetooth of Denmark, who united warring Danish tribes into a single kingdom. Marketing Bluetooth as a standard communication protocol that everyone could adhere to and follow was a good decision. The Bluetooth logo is a bind rune merging the Germanic runes H (Hagall) and B (Berkanan) for Harold Bluetooth.

The Bluetooth SIG (special interest group): the Bluetooth SIG is a group of companies which take care to maintain the standards and licensing agreements involved with Bluetooth. The special interest group has companies participating from different industries, all of whom think that Bluetooth will make a difference to the way they do business.

Bluetooth Logo

After 1997, Ericsson began talking to different companies, insistent on creating a new global standard for communication. They sought to bring together market leaders in mobile telephony, portable computing, digital signal processing, everyone who could help make Bluetooth the household phenomenon it is today. In 1998, it tied up with Nokia, IBM, Toshiba and Intel. They held simultaneous press conferences to announce that they were developing a licence-free, open specification for wireless communication, and the idea took off. The Bluetooth SIG is responsible for maintaining the

Bluetooth specification. In 1999, the first version of the Bluetooth specification was released, around 1,500 pages in length, detailing exactly how to utilise Bluetooth for every-day purposes. In 1999, 3Com, Lucent Technologies, Microsoft and Motorola joined as promoter members. Other businesses can join the Special Interest Group at an associate or adopter level. Since Bluetooth is pertinent across industries, almost all of them have a vested interest in the success of this initiative.

The Bluetooth specification: the Bluetooth specification contains all relevant details about Bluetooth, from the technical aspects, to licensing and marketing products with the Bluetooth logo. It is divided into two parts: volume 1 (Core) and volume 2 (Profiles). The entire 1,500-page document is available from the Bluetooth SIG Web site, at **www.bluetooth.com/developer/specification/specification.asp**.

Volume 1 specifies different components and protocols of the Bluetooth wireless technology. Very detailed technical information about the following is included:

- The protocol stack–including core protocols, the Cable Replacement protocol, the Telephony Control protocol, and several adopted protocols.
- The Bluetooth radio.
- The link manager.
- The transport layer.
- Interoperability between different communication protocols.
- Testing and compliance.

The second volume of the Bluetooth specification handles “usage models” and “profiles.” A usage model is a specific type of Bluetooth application, such as a three-in-one phone, an internet bridge, a sync between your gaming console and your phone, Bluetooth on your mp3, and all other specific technologies. A profile is the detailed technology and procedures required to implement a particular application. Profiles specify exactly how the Bluetooth protocol stack is to be used, how the options can be reduced, and how procedures can be used from several standards. Profiles define a common user experience for that particular type of use. All Bluetooth devices must be tested against one or more appropriate profiles in order to be certified. As long as the qualifications set by the Bluetooth SIG are met, as specified in the Bluetooth specification, products are licensed to use the Bluetooth technology and the Bluetooth brand and logo at no charge. This allows an open standard which can reach out to a broad market base. Inter-compatibility with various other electronic devices also allows for mass consumer acceptance of this technology.

How Bluetooth works: Bluetooth uses radio frequency (RF) signals to establish a point-to-point and point-to-multipoint voice and data transfer. The term that best explains the networks created is a personal area network. Bluetooth-enabled devices within a range of 30 feet (10 metres) form a piconet, an ad hoc wireless network where communication occurs via RF signals. For a device to communicate with another, both must contain a Bluetooth radio. The radio, which is extremely small, is actually built into a computer chip which manages the individual connections. The radio also consumes very little power. Every Bluetooth radio conforms to the exact same specifications for both transmitting and receiving signals, so that they can be used anywhere in the world without modification. Bluetooth devices can also link through a series of piconets to larger local area networks, and the global internet.

Bluetooth was developed by Ericsson to connect earphones to your mobile phone without wires

Bluetooth simplified connections across electronic devices for two reasons. One - wireless connectivity. Two – it initiated a global standard with every Bluetooth device following similar specifications and communication protocols. Be it with wires or without, connecting two different devices made by different manufacturers can be quite a complex procedure. The simplest example is that of the mobile charger, different companies have different pins (though there is talk of a soon to be released universal charger). In the wired world, creating the proper physical connection is sometimes quite challenging. Plugs, pin to pin connectivity, various connectors – serial, parallel, optical and so on – the choices are mind boggling. Beyond that, there's serial communication where data is sent one bit at a time, and parallel processing, where data is processed in groups of 8 or 16 bits. The Bluetooth specification therefore bypasses all these troubles, and this is one of the main reasons for its widespread success.

The first part of the Bluetooth standard dictates that all devices connect via a specific set of radio frequencies. The rest of the Bluetooth standard explains the precise protocols used to transmit and receive data over the wireless connection. All Bluetooth devices must use the same protocols, so they all talk the same electronic language.

We have mentioned that Bluetooth transmits data using radio frequency and using a low-frequency portion of the electromagnetic spectrum. TV Stations and FM Radio stations also use that portion of the spectrum.

In the earlier portions of this Fast Track, we've already mentioned how radio signals work and how data can be transmitted wirelessly, so we shall avoid going through it again. Bluetooth uses the 2.40 GHz to 2.48 GHz band. That is, the Bluetooth Radio transmits and receives data at a frequency of 2.40 GHz (gigahertz). Unlike infrared transmissions, which use light waves and require connecting devices to be in sight of each other, radio waves have no line-of-sight requirements and can, in fact, pass through most solid objects. This means that a Bluetooth radio can transmit its RF signals from inside a briefcase, or through office walls. The frequency around the 2.40 GHz band is termed the ISM band (for industrial, scientific and medical purposes). It is free for anyone to use, for any purpose. The benefit of such free licensing is that it allows for experimentation with free communication techniques. The disadvantage is that it leads to crowding of the spectrum since space within the band is finite, and several other devices also use it. Both voice and data communication via Bluetooth utilise this portion of the spectrum.

Bluetooth doesn't need the devices to be in the line of sight, unlike earlier infrared systems

Currently, the 2.4-GHz band is used by devices such as cordless phones, some urban and suburban wireless communication networks, 802.11 wireless networks and microwave ovens, among others.

So, if you use a Bluetooth device in and around other emissions which use the same spectrum, the other devices can effectively "jam" your device's transmissions.

To avoid interference, which seems inevitable considering the host of devices using the same band, Bluetooth radios utilise a technique called spread spectrum frequency hopping (also known as frequency-hopping spread spectrum, FHSS). This is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. Splitting the signal across various frequencies as opposed to keeping it on a fixed one allows for three major advantages. One, it reduces narrowband interference. During the recollection process of the spread signal, the interfering signal is also spread, which allows the receiver to eliminate it as it disappears into the background. Two, spread signals are difficult to intercept considering they are scattered across various frequencies in a pseudo-random order. For any eavesdropper, it would appear as noise unless the exact order of scattering of the signal was known. Three, a spread spectrum transmission can share a frequency band with most other signals with minimal interference. It also adds minimal noise to narrow frequency communications. This improves the efficiency of bandwidth utilisation.

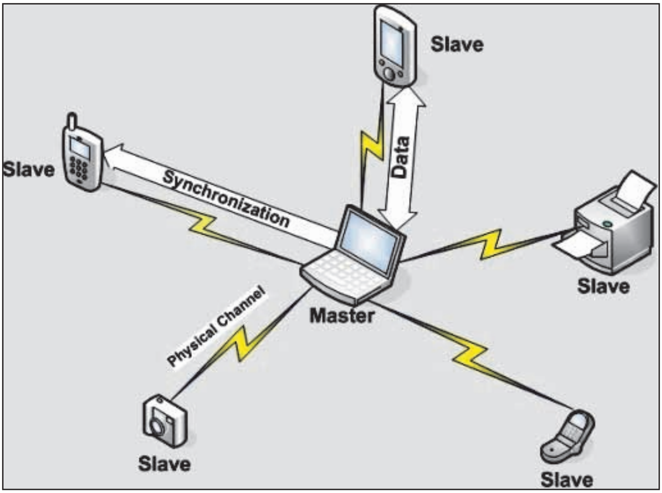
Bluetooth devices are more efficient than other wireless devices utilising the spectrum due to faster hops and shorter packets

For easy transmission of data, to avoid large losses, data is typically broken up into very small parts, called packets. FHSS isn't a new technology, but Bluetooth is more efficient than most other devices utilising the spectrum since the devices typically hop faster and use shorter packets. All Bluetooth devices are capable of transmitting both voice and data signals.

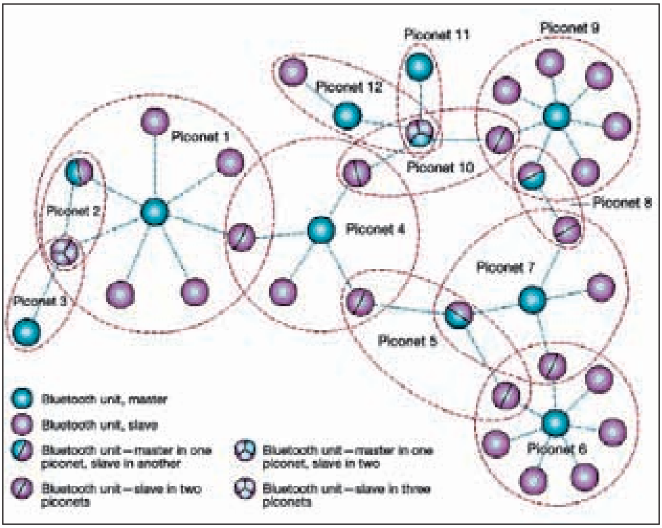
Any two Bluetooth enabled devices that come within 30 feet of each other can set up an ad hoc point to point or point to multipoint connection. So, as you travel, your personal network travels with you. There are two major states of operation in a Bluetooth device, connection and standby. If a device is connected and not actively involved with current activities, then standby mode is triggered. This acts as a power conservation technique in Bluetooth devices. If a device is on standby, it waits for active connections. Hence, it "listens" every 1.28 seconds, for messages from other devices. Again, as mentioned before, Bluetooth prefers to access a range of channels, and the listening takes place across 32 hop frequencies for that specific type of unit. As mentioned earlier, the Bluetooth Specification has exact listings for each "profile", hence mobile phones will search across a different range of frequencies compared to other devices.

The concept of a master-slave is set up once one unit senses another Bluetooth device in the region. The first device that found the other unit assumes the role of the master unit in the development of the piconet. Of course, since all Bluetooth radios are identical, any unit may assume the role of the master or the slave. The only cause for selection is which detects the other first.

When two Bluetooth devices establish a connection, they have created a type of personal area network called a piconet. Each piconet can contain up to eight different Bluetooth devices. Within each piconet, one device serves as the master, while the other seven devices function as slaves. Any individual device can



Piconet


Piconet 11
Piconet 9
Piconet 12
Piconet 1
Piconet 10
Piconet 2
Piconet 8
Piconet 4
Piconet 7
Piconet 3
Piconet 5
Piconet 6
Bluetooth unit, master
Bluetooth unit, slave
Bluetooth unit—master in one piconet, slave in another
Bluetooth unit—slave in two piconets
Bluetooth unit—master in one piconet, slave in two
Bluetooth unit—slave in three piconets

Scatternet

belong, simultaneously, to multiple piconets.

There are a few limitations with the piconet systems. Only three of them at a time can carry full-duplex voice transmissions. All the devices in a piconet share the same frequency-hop channel, which is established by the slaves synchronising their internal clocks to the master unit's clock. All piconets have a unique identity and thus multiple piconets can share the same physical space without interference.

To connect more than eight devices at one time, multiple piconets need to be created, and then all the master devices need to be connected together. Such a combination is a called a scatternet.

Since Bluetooth uses 79 frequencies in total, a maximum of 10 piconets with 80 different Bluetooth devices can be included in any single scatternet. Beyond this number, saturation is reached.

However, multiple piconets that share the same physical space do not have to be connected to one another and can continue to operate independently without interference since each operates on a different frequency hop-channel.

Both piconets and scatternets are types of networks that are established in an ad hoc fashion. In an ad hoc network, all devices in the network are treated as peers. Even though one device in a piconet will assume the role of master, that role could be assumed by any device, and can be swapped between devices if and when necessary.

Let's compare that to a more structured type of network such as a cellular phone network.

In a typical cellular network, base stations (or transmitters) are placed at strategic positions to provide local cell coverage, while cellular phones (or radios) are used to connect via radio link to the base stations. With a cellular network, there is a strict and permanent separation between the base stations and the terminals. A cellular phone can never function as a base station, and vice versa; only the base station can provide channel access, allocate channels, control network traffic, and otherwise manage the flow of signals through its particular cell.

The advantages of an ad hoc network are many. First, there is no need to establish a costly infrastructure to service a particular geographic region – ad hoc networks are formed on the fly, where the devices are, without the need for base stations to control network communications. Second, unlike cellular networks, multiple ad hoc networks can occupy the same physical space without fear of interference. Third, any Bluetooth unit can "control" an ad hoc piconet as a master device; no special control devices (or operators) are necessary.

So we have now discussed the basics of Bluetooth and how communications are done. There are few issues with Bluetooth connectivity and ad-hoc networks that need to be discussed.

Ad hoc networks don't need costly infrastructure, thereby reducing cost

The most important is the question of security. One question that has has often been raised is just how secure are these connections? What's to stop someone else's Bluetooth device from picking up your personal signals. For businessmen at crowded locations, or anyone else for that matter that considers their data valuable and needs security, Bluetooth could be a mistake. However, the Bluetooth specification ensures that devices have a 128-bit key. That, combined with a cipher for encryption, ensures that a Bluetooth device is as secure as a wire-based connection. However, this still does not prevent data theft.

Another rather creative use of these Bluetooth networks is for viral advertising or campaigning which has come to be called Bluetooth hijacking or Bluejacking. Bluejacking involves Bluetooth users sending a business card, text message, audio, video or other data to other Bluetooth users within a 10-metre radius. If the user doesn't realise what the message is, he might allow the contact to be added to his address book, and the contact can send him messages that might be automatically opened because they're coming from a known contact. Most Bluetooth users don’t suspect this and it has been used successfully for viral advertising. Bluesnarfing is a term given to Bluetooth hacking. The downside to Bluetooth popularity is that there are a lot of viruses, malware and trojan horse programs that can infect and attack Bluetooth devices.

Bluejacking

5.2 Bluetooth versions

Since the creation of Bluetooth in 1994, and its subsequent marketing post 1997, several strides have been made in development.

As one might expect, the first Bluetooth versions 1.0 and 1.0B had quite a few problems, especially when it came to inter-operability between different manufacturers of electronic devices.

Bluetooth 1.1 was ratified as part of IEEE Standard 802.15.1-2002. The IEEE is an international organisation for electronic and electrical engineers and is often responsible for initiating standards and protocols. The errors in 1.0B Specification were fixed and there was added support for non-encrypted channels. An indication of the strength of the Bluetooth signal also called

Received Signal Strength Indicator (RSSI) was added.

Bluetooth 1.2 was backward compatible with 1.1. Backward compatibility means that anything that worked on Bluetooth 1.1 would definitely work on 1.2 although the reverse need not be the case.

The major improvements were:

- Faster connection and discovery
- Adaptive frequency hopping spread spectrum (explained earlier: how a signal is transmitted across various frequencies for better noise reduction and interference
- Better transmission speeds
- Improved voice quality
- Checked and ratified as IEEE Standard 802.15.1-2005

Bluetooth 2.0 was released on November 10, 2004. Backward compatibility was ensured and the main change was faster data transfer by introduction of an enhanced data rate. Using a combination of various different radio technologies, Gaussian frequency shift keying (GFSK) and phase shifting keying (PSK), it managed to improve the data rate. The 2.0 specification allows for benefits such as more than three time the transmission speed, reduced complexity in case of multiple simultaneous connections, and lower power consumption. The EDR is an optional feature.

Backward compatibility with earlier versions ensures older Bluetooth devices will continue to function with newer devices

Bluetooth 2.1 was released on July 26, 2007 and the following features were added. In non-technical terminology, the benefits were:

- Better filtering of devices before connection using a more sophisticated method of collecting information about the device, its manufacturer and other details.
- Lower power consumption when not engaged in active transmission and waiting and searching for nearby Bluetooth devices. This specially benefits wireless keyboard and mouse devices as it increases their battery life by letting

the devices decide how often to communicate with each other.

- Better encryption management facilities.
- Improved strength of security in paired connections.
- Near field communication cooperation. NFC is another wireless technology with a very small range of around 10 centimetres or 4 inches. It allows for the creation of automatic secure Bluetooth connections when NFC radio interface is available. An example is the automatic uploading of photos from a mobile phone to another device just by bringing it close to the electronic device.

Bluetooth 3.0 is the newest specification adopted by the Bluetooth SIG (Special Interest Group) on April 21st 2009. The main feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport system. UWB (ultra-wideband) is missing from the specification. 802.11 is associated with Wi-Fi and alternate MAC/PHY or AMP allows the use of alternate MAC and PHYs for transporting Bluetooth profile data. The conventional Bluetooth radio is still used as the primary device for device discovery, initial connection and profile configuration, but the AMP option is used for high speed data transfer, especially when a great deal of data needs to be sent. 3.0 also allows for faster connections for small data by passing few protocols and for more standardised encryption key sizes.

Bluetooth saves power effectively, and in turn improves efficiency

The newest rage in Bluetooth technology is the Bluetooth low energy technology. This is an additional protocol stack added to the Bluetooth specification, and it is compatible with existing stacks. Earlier similar attempts, such as Wibree and Bluetooth ULP (ultra low power) have been outdated with the introduction of low energy. Bluetooth low energy technology is an open radio technology for really small devices. It addresses devices with very low battery capacity and is easily integrated with traditional Bluetooth. People are aware that this has great implementation opportunities for applications such as medical instrumentation. Imagine a small micro-circuit enabled with

Bluetooth technology monitoring your heartbeat wirelessly.

The advantages are obvious – lower power consumption and longer battery life. It could be very useful for many kinds of sensors. Though no final product release has been fixed and the technology has not been made commercially available, the need in the market for such technology is significant. The major difference is that the speed available for data transfer will be limited and there is no voice capability. However, the advantages offset these limitations, as sensors are getting smaller and smaller and cannot depend on wires to connect them to monitors.

To promote these ideas and the development of Bluetooth technology with increased focus on low energy, the Bluetooth SIG has opened up registrations for the Bluetooth Innovation World Cup, an open platform where aspiring innovators can submit their ideas. Since the focus is on low energy, the ideas are primarily focused on sports, medical and fitness products.

Bluetooth is now setting foot into health, fitness and sports applications

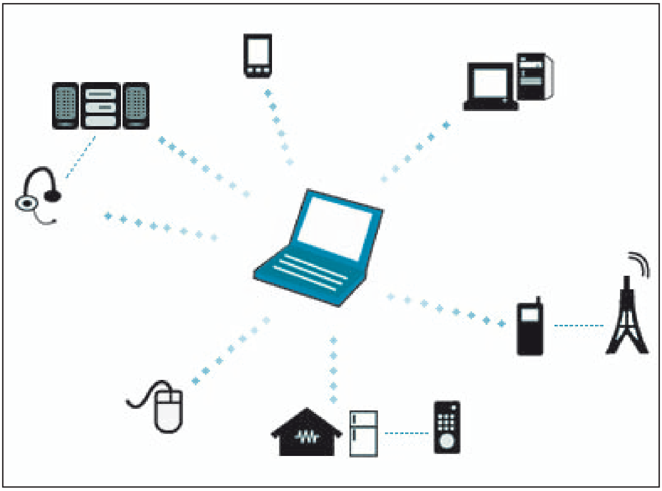
There are, of course those who feel that the Innovation World Cup is more of a marketing initiative as opposed to a technical enterprise.

Bluetooth devices: today Bluetooth technology has permeated almost every kind of electronic device. The potential for the imagination is considerable. However, there are a few basic models on which all Bluetooth devices are built. These are enlisted in the Bluetooth specification in the profiles. Basically, Bluetooth profiles are specifications that devices must follow. The various features in Bluetooth profiles are provisions for:

- Audio streaming (from Radio to headset).
- Cordless telephony (transmitting signals from a landline to a wireless headset).
- Audio video remote Control (controlling your TV and other A/V devices).
- Dial-up networking (connect to the internet).
- Fax option (linking to a fax machine).
- File transfer capabilities (share files with people around you).
- Copy cable replacement profile (allows you to replace

wires with Bluetooth connections – very generic, hence drivers need to be installed for specific case scenarios).

- Hands-free profile (used when talking on mobile phones in cars).
- Human interface device profile (HID – used for providing support for mice, joysticks and keyboards). Playstation 3 controllers and Wii remotes use Bluetooth HID.
- Headset profile (for mobile phones and headsets).
- Intercom profile or the walkie-talkie profile for voice calls between two Bluetooth capable handsets.
- LAN access profile (LAP – for connection over Bluetooth to LAN, or, local area network, WAN, wide area network or the internet). Of course, there needs to be a device that is physically connected to the network.
- Object Push Profile for sending pictures, virtual business cards, etc.
- Personal area networking profile – piconets have been discussed earlier.
- Phone book access profile allows for access to phone book data which gives callers or users involved in data transfer more information.



Bluetooth devices

- SIM access profile allows devices such as car phones with built in GSM receivers or transmitters to connect to any SIM card in a phone which is Bluetooth enabled, so the car phone itself doesn't require a separate SIM card.
- Video streaming (from cameras to other devices).

There are a few more but these are the most generically useful ones. The Bluetooth specification is of course edited and ratified quite frequently, and hence there is the possibility of additions.

5.3. Enabling Bluetooth on your computer

WORKSHOP : Using Bluetooth on your PC

Since Bluetooth is a relatively new technology, in case you bought your desktop a few years back, chances are you don't have Bluetooth compatibility. However, that is not a major problem. Today, you can buy a separate device that will allow you to access Bluetooth from your desktop. For our demonstration, we'll assume that you have a Broadcom Bluetooth device and Windows XP SP2 (Service Pack Two).

A personal computer must have a Bluetooth adapter in order to communicate with other Bluetooth devices such as mobile phones or wireless support for keyboards and mice. If yours does not have a pre-installed Bluetooth adapter, you will have to get one in the form of an external dongle – this is a small piece of hardware. Most Bluetooth adapters come with a USB device, so you will have to connect it to a USB port. Bluetooth allows multiple devices to communicate with a computer over a single adapter.

A Bluetooth stack is the technical term for the implementation of the Bluetooth protocol. Widcomm made the first stack for Windows. It was later acquired by Broadcom.

Bluetooth dongle

Windows did not support Bluetooth until Windows XP Service Pack 2 – all later versions have Bluetooth support and native drivers. Apple has supported Bluetooth since Mac OS X v.10.2 which was released in 2002.

Linux has two popular Bluetooth stacks, BlueZ and Affix. BlueZ was developed by Qualcomm and Affix by Nokia.

Now, many companies provide Bluetooth dongles. Microsoft also has its own hardware. We recommend you go to the closest electronics shop and enquire what is readily available. A good range is necessary. Hence choose your Bluetooth hardware according to your requirement. You should consider a few factors such as the size of your house, the possibility of interference, etc. We have also mentioned a few profiles earlier on, so based on why you need Bluetooth, you should ensure that the hardware supports all profiles. Most do.

What you need:

- Desktop PC with Windows XP Service Pack 2 installed.
- A Bluetooth dongle (usually in the form of a USB stick).
- Driver installation file – check out native support in case of laptop drivers. There are several internet locations for downloading Widcomm/Broadcom drivers.
- BFor specific software purposes, download the required software – we shall not be dealing with this as it might vary from user to user. e.g. the Nokia PC Suite for specific Nokia support for Bluetooth.

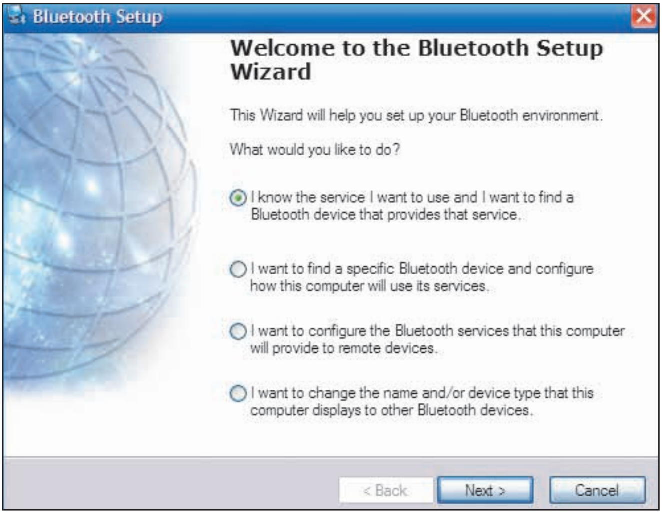
Basic preparation

- Log on to Windows with administrative rights.
- Ensure your firewall is turned off .
- Disable antivirus if required.

Insert the Bluetooth device into the USB Slot. If your computer detects it automatically, you are lucky. In that case, you need not bother installing the driver as it is pre-installed.

If it does not detect it, you do not yet have Bluetooth support, so install the drivers. But before installing the driver, ensure that the Bluetooth device is not plugged into the USB port. Also ensure that all earlier software which is similar is uninstalled. Installers usually take care of this feature.

Extract the required files and install them. All installers



Bluetooth Setup

Welcome to the Bluetooth Setup Wizard

This Wizard will help you set up your Bluetooth environment.

What would you like to do?

● I know the service I want to use and I want to find a Bluetooth device that provides that service.

○ I want to find a specific Bluetooth device and configure how this computer will use its services.

○ I want to configure the Bluetooth services that this computer will provide to remote devices.

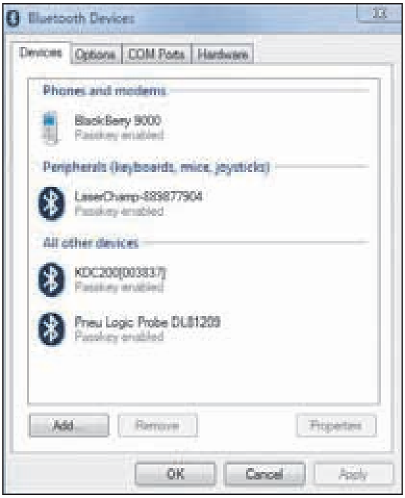
○ I want to change the name and/or device type that this computer displays to other Bluetooth devices.

Bluetooth setup wizard

come with specific step by step instructions. Following them should be sufficient. In most cases, agreeing to the terms and conditions and clicking next should get you through it.

After installation, you might be expected to restart your computer. Plug in your USB drive. If you then see a blue icon on your taskbar with a white Bluetooth logo, you're good to go. In case there is no connectivity, your icon will feature the Bluetooth logo with red instead of white.

You can use the Bluetooth wizard



Bluetooth Devices

Phones and modems

BlackBerry 9000
Passkey enabled

Peripherals (keyboards, mice, joysticks)

LaserChamp-889877904
Passkey enabled

All other devices

KDC200[003837]
Passkey enabled

Pneu Logic Probe DL81209
Passkey enabled

Bluetooth device options

for generic changes. The wizard will take you through a set of specific instructions for performing standard tasks. For more options, you will have to access the control panel.

You can use the Bluetooth Devices item in Control Panel to configure Bluetooth settings. By using Bluetooth Devices, you can do one or more of the following:

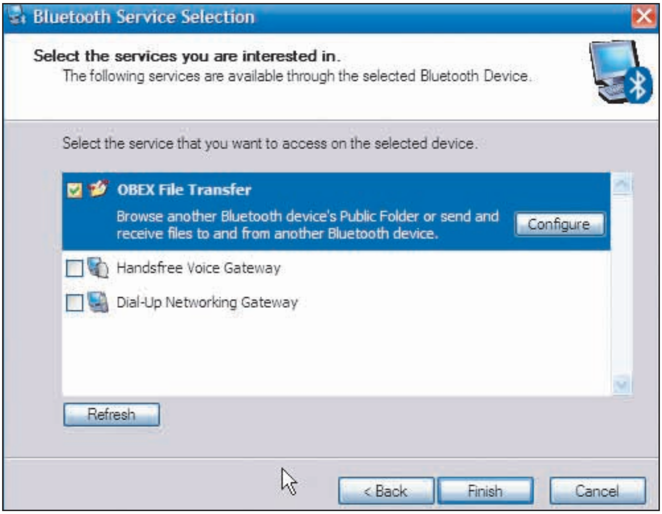
- Add or remove a device.
- View the properties of a device.
- Change your Bluetooth options.

When you view the properties of a Bluetooth device, you see the following information:

- The device type
- The hardware address of the Bluetooth adapter
- The date and time of the last connection
- Information about whether a passkey is used for pairing with the device.

You can also change the name that Windows uses for the device.

The Services tab shows information about the services that the device supports. This tab may also show internet dial-up networking connections. Hardware synchronizations and COM port support are also available. You can also select the services



Select the services you are interested in.
The following services are available through the selected Bluetooth Device.

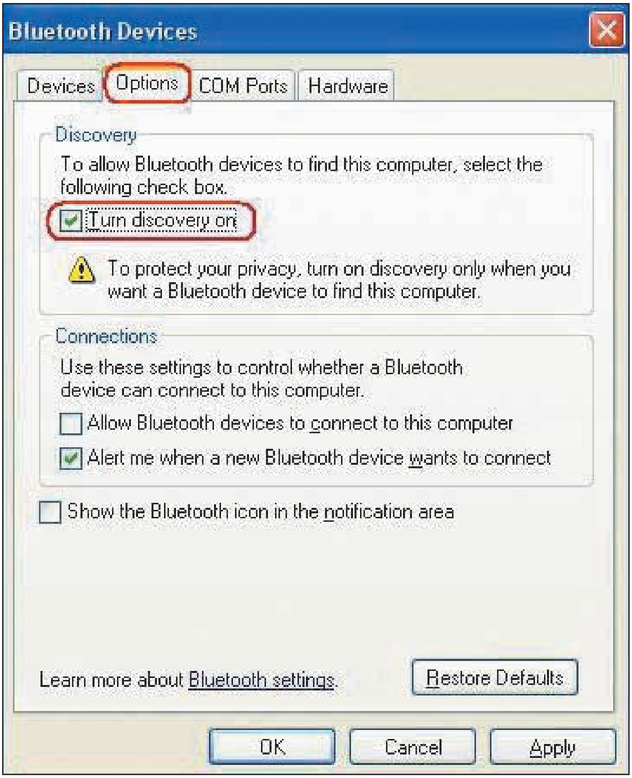
Select the service that you want to access on the selected device.

☑ **OBEX File Transfer**
Browse another Bluetooth device's Public Folder or send and receive files to and from another Bluetooth device.

□ Handsfree Voice Gateway

□ Dial-Up Networking Gateway

Service selection



Discovery

To allow Bluetooth devices to find this computer, select the following check box.

☑ Turn discovery on

To protect your privacy, turn on discovery only when you want a Bluetooth device to find this computer.

Connections

Use these settings to control whether a Bluetooth device can connect to this computer.

☐ Allow Bluetooth devices to connect to this computer

☑ Alert me when a new Bluetooth device wants to connect

☐ Show the Bluetooth icon in the notification area

Learn more about Bluetooth settings.

Turn discovery on

that you want to use.

The Options tab in Bluetooth Devices provides the options that control how devices discover and connect to your computer. The main option is "Turn discovery on". This option lets devices discover your computer so that you can make a connection.

Other options on this tab include the following:

- Allow Bluetooth devices to connect to this computer. If it is cleared then others cannot connect to your machine.
- Alert me when a new Bluetooth device wants to connect. This gives you an alert when another device tries to connect to you (just in case you want to block it). If cleared, no

notification is given.

Of course, the entire case is academic in case the first "Allow Devices to connect" is unchecked.

Other options on the Options tab let you turn on or turn off the Bluetooth icon in the notification area and restore default settings.

Typically, your Bluetooth enabled computer will discover other devices. Therefore, you only have to turn on the Turn Discovery On option when your computer acts as a device. For example, you might want to turn on this option when your computer is connected to another computer by a Personal Area Network (PAN). When computers are connected by a PAN, one of the computers must have discovery turned on.

By default, discovery is not turned on in Windows XP SP2, because a discoverable Bluetooth device may be less secure than a device that is not discoverable. We recommend that you keep the Turn Discovery On check box cleared unless you want another Bluetooth device to discover the computer. When the connection is complete, the Add Device Wizard turns off discovery automatically.

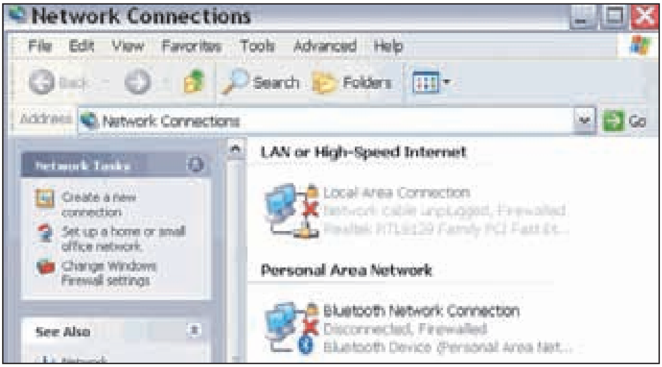
Joining a personal area network

Personal Area Networking (PAN) provides ad hoc networking between Bluetooth devices. All devices that you want to network must support PAN in order to create a PAN network. To join a PAN network, you can use any one of the following methods:

- Click the Join a Personal Area Network option in the Bluetooth taskbar icon menu.
- Double-click the Bluetooth Network Connection icon in the Network Connections item in Control Panel.
- Click View Bluetooth network devices in the Network Tasks pane in Network Connections.

Each of these methods opens the Bluetooth Personal Area Network Devices dialogue box. This box displays a list of devices to which you can connect. You can also add or remove devices from this list by using the options at the bottom of the dialogue box.

To make a connection, select the device that you want to connect to, and then click Connect. When the connection is complete, TCP/IP networking is available between your


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
See Also
Network

LAN or High-Speed Internet

Local Area Connection
Network cable unplugged, Firewalled
Realtek RTL8139 Family PCI Fast Et...

Personal Area Network

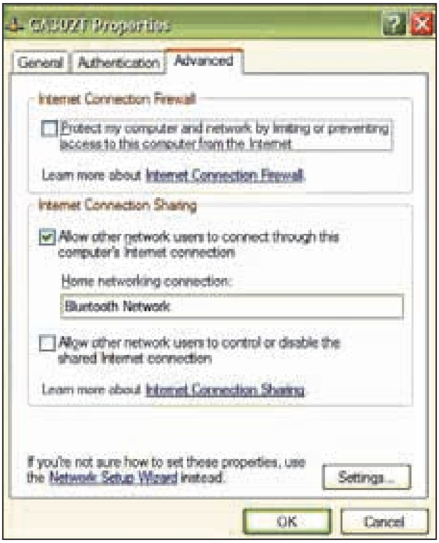
Bluetooth Network Connection
Disconnected, Firewalled
Bluetooth Device (Personal Area Net...

Join a personal area network

computer and the other device. (If you click a device to which you are already connected, the Connect button becomes a Disconnect button.)

There are several other features you can utilise. Check the Windows Help page on the internet for detailed support on Bluetooth. You may bridge other Bluetooth devices and allow them to use the internet from your comp, you may want to initiate data transfer from one machine to another machine etc.

For most devices enabled with Bluetooth, such as mobile phones, there are specific software connectivity suites. In the case of wireless mice and keyboards, there are different configurable



Internet Connection Firewall

☐ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

Home networking connection:

Bluetooth Network

☐ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

Allow other computers to access the internet options such as Sleep Mode, etc. We recommend you try these options out yourself depending on your Bluetooth device.

5.4 The future of Bluetooth

So how can *you* use Bluetooth? Bluetooth can be used in the following ways.

- All computer peripherals are wireless – wireless mouse, joystick, keyboard, modem.
- Your digital camera is synced wirelessly with the computer.
- The mobile phone is Bluetooth enabled allowing you to access your computer for information, sync with the digital camera for transferring pictures. Access your phone book via Bluetooth.
- Access the internet wirelessly by syncing your laptop to your modem in another room.
- The lights in your room, you TV, your a/c – can all be synced together, with one remote allowing you control of your household environment.
- Imagine an "intelligent house" with everything in your control at the touch of one remote control – enabled with Bluetooth. That is the future.
- Cars are also becoming increasingly reliant on Bluetooth technology.
- The future of Bluetooth may include heavy reliance on Bluetooth technology for mobile commerce as well. Paying at a ticket counter, the line at your store, a pay-and-park? All are possible using Bluetooth.
- A few more initiatives are being undertaken to transfer power wirelessly – something many people believed was impossible. Once that is accomplished, you be able to charge your mobile phone wirelessly!
- Today, Bluetooth has been able to combine with Wi-Fi technology as part of the Bluetooth 3.0 specification. It can access 3G and WiMax networks. The short range of <10 metres is also increasing. Better telephony, better connectivity, better communication.
- Bluetooth allows new age technology to sync. Recent news reports show how the Apple iPhone and the Nintendo Wii can now be linked together using Bluetooth. So talk, game, communicate, share pictures and connect to the internet. All

simultaneously, with Bluetooth being the bridge that links them all.

- The Bluetooth SIG is also promoting UWB, or ultra wideband, which will allow faster access and higher data transmission rates.
- The Bluetooth Low Energy Technology has great potential in micro-sensors.

So using Bluetooth, there's connectivity, communication, entertainment, health, commerce, plus a great deal of untapped potential in several other sectors. Of course, there's always competition: from different wireless technologies to companies such as Logitech creating their own technologies that allow for an easier sync between their own products. It's Bluetooth's advantages that differentiate it from others – it's free and it does not consume much power. Wireless technologies are here to stay, and though Bluetooth may be a relatively late entrant, it has made its mark and should survive.

Wi-Fi

6.1 Introduction and history

Wireless is obviously no longer a stranger to most people. Even for someone unacquainted with the concept of RF transmissions or any mode of wireless communication, Wi-Fi would not be a new term. Almost every individual who owns a laptop would probably have been witness to a Wi-Fi signal once in a while. Even in a country like India where wireless zones aren't really as popular as in the west, there are several housing societies, corporate houses, and educational institutions who have access to Wi-Fi – your portal to wireless internet. Today, Wi-Fi is synonymous with WLAN (Wireless Local Area Networks) in most countries. Its uses are versatile and its technology quite established and prolific. Through the course of this chapter, we shall describe the history of Wi-Fi, the basic overview of its working, the devices that operate it, the features it offers to users, the potential it has, the security issues regarding Wi-Fi and how you can enable wireless networking on your computer.

History

Wi-Fi is part of radio technology, where data is transmitted using radio waves of high frequency. As mentioned before, there is a part of the electromagnetic spectrum which is unlicensed. Anyone can utilise that part of the spectrum for their purposes. This unlicensed spread spectrum was first available in the USA in 1985. The Federal Communications Commission laid down stringent regulations for usage of the spectrum which was later implemented in most other countries as well. The spectrum was intended for civilian usage, and is responsible for almost all free wireless technology currently available.

With the growth of Wi-Fi, the term is now synonymous with wireless LAN

The precursor to Wi-Fi was invented in 1991 by the NCR Corporation and AT&T in the Netherlands. Intentionally meant for cashier systems, the first wireless products were introduced under the term WaveLan with speeds of 1-2 Mbit/s. Vic Hayes is known as the 'father of Wi-Fi' as he was actively involved in the design of standards such as IEEE 802.11b and 802.11a. IEEE is the Institute for Electrical and Electronics Engineers. It is a global non-profit professional organisation which, apart from publishing research work, fostering innovation and educational activities, also establishes international standards for electrical and electronic technology. The IEEE 802.11 is a set of standards which sets rules and protocol for wireless local area network communication in the 2.4, 3.6 and 5.0 GHz frequency bands.

The Wi-Fi Alliance owns the trademark for Wi-Fi

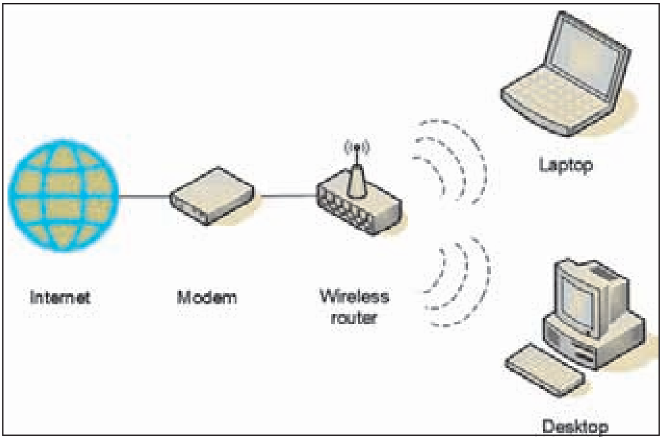
The original patents for the Wi-Fi technology were filed in 1996 and are held by CSIRO, a research body in Australia. However, it gave way to several legal battles over non-payment of royalties between the research organisation and other major IT corporations. A settlement was reached in 2009, but the resolution was not revealed to the public. The Wireless Alliance is a body of several companies. It promotes standards aimed at improving the inter-operability of wireless LAN products based on the IEEE 802.11 standards, much like the Bluetooth Special Interest Group. The term Wi-Fi was first commercially used in August 1999 by the Wireless Alliance as it was considered more cool and catchy than the more technical IEEE 802.11b Direct Sequence. The term suggests Wireless Fidelity, in comparison with audio recording term High Fidelity, or Hi-Fi, as an indication of quality. Though the term Wireless Fidelity has been used in an informal way, the actual term Wi-Fi does not actually mean much. A look at the Yin-Yang logo for the Wi-Fi group also suggests the stress they lay on interoperability. The Alliance has however downplayed the link to Hi-Fi and now focuses on it being "a standard for wireless fidelity" and really just another brand name.

Wi-Fi Alliance: the Wi-Fi Alliance is a trade group that has the rights to the trademark Wi-Fi. Formed in 1999 in order to maintain compliance with IEEE 802.11 standards, the Wi-Fi Alliance monitors, tests and attests product and specification compliance to the IEEE standards for all electronic products using the technology. The early 802.11 products suffered from interoperability since IEEE had no provision for testing equipment. The IEEE 802.11b saw companies endorsing the specification and witnessed the formation of the Wireless Ethernet Compatibility Alliance (WECA) and branded the technology Wi-Fi. The group of companies included 3Com, Cisco, Intersil, Agere and Motorola. The list of course details their current names and not the names the Alliance was formed under. The organisation was set up in order to perform testing, certify the inter-operability of electronic devices claiming adherence to 802.11 specifications and promote the technology as a whole. It was renamed the Wi-Fi Alliance in 2000. The Alliance owns and controls the prolific Wi-Fi certified logo, a registered trademark that is permitted only on tested equipment. The rigorous certification process ensures high adherence to brand standards, reliability, security and interoperability.

Wi-Fi Alliance

The focus is on:

- Compatibility and interoperability where the product being tested is tested for connectivity with other certified equipment. Testing is done with multiple devices from different equipment manufacturers.
- Conformance to standards and backward compatibility. Since technology keeps evolving, it is essential that all new technology is perfectly compatible with its earlier versions. High adherence and conformance to the 802.11 standards is also essential.
- High performance standards in order to meet end user requirements. Each product must maintain certain minimum standards in order to be certified by the Wi-Fi Alliance. Specific performance test results are however, not released by the Alliance to the public.



Wi-fi transmissions from one system to another

6.2 How Wi-Fi works

Transmission of Signals: Wi-Fi is a wireless network enabling technology that uses radio waves. We've covered RF transmissions and how to send and receive basic radio signals in the earlier chapters of this Fast Track and hence we shall avoid pursuing this further here. Wireless communication across Wi-Fi is a lot like the standard two-way radio communication.

First, the wireless adapter of a computer translates data into a radio signal that it transmits using an antenna. Then, a wireless router receives the signal and decodes it. The decoded information is sent to the internet using a physical, wired Ethernet connection. Of course, the reverse process is also duly carried out. The radios for Wi-Fi communication broadcast and receive at frequencies of 2.4 GHz or 5.0 GHz. The 2.4 GHz spectrum is the ISM spectrum (industrial, science and medical usage) and is an unlicensed part of the electromagnetic spectrum. Both 2.4 GHz and 5 GHz are much higher than the standard frequencies used for cell phones and other wireless devices. The higher frequency allows the signal to carry more data.

The way data is transmitted depends on the protocol and specifications of the device. Since all Wi-Fi devices use the same 802.11 protocols, they should be compatible and interoperable.

When connecting any two devices, whether by cable or wirelessly, care should be taken such that both sender and receiver encode, transmit, and decode data in a similar fashion.

Wireless networking has several standards. The 802.11a standard transmits at 5.0 GHz and can move up to 54 megabits of data per second (around 6.75 MBps transfer speeds). The original Wi-Fi protocol 802.11 used a DSSS (direct sequence spread spectrum) modulation technique. In DSSS, a noise signal is multiplied along with the signal and scattered across a wide band of frequencies. The noise signal is a random sequence of + (plus) and – (minus) ones, synchronized between both sender and receiver. The frequency of the original signal is multiplied, spreading the energy to a wider band. The 802.11a improves on this and uses OFDM (Orthogonal Frequency Division Multiplexing), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.

While the 802.11b is the slowest, the newest version 802.11n is the fastest and will be available soon

The 802.11b standard is the slowest, but is also the least expensive standard. 802.11b transmits in the 2.4 GHz band of the spectrum. It can handle only up to 11 megabits per second (as little over one MBps) and it uses complementary code keying (CCK) modulation to improve speeds. Complementary codes are sets of finite sequences of equal length. They are generated such that the number of pairs of identical elements with any given separation in one sequence is equal to the number of pairs of unlike elements having the same separation in the other sequences.

The 802.11g standard transmits at 2.4 GHz, like 802.11b, but it's a lot faster as it can handle up to 54 megabits of data per second. 802.11g is also faster because it uses the same OFDM coding as 802.11a.

802.11n is the newest standard that is due to become widely available. The standard significantly improves the speed and range of Wi-Fi devices. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. The standard is currently in draft form and is rumoured to be due for release by 2010.

Once the signals can be received and sent using a similar protocol, a wireless network can be established between two Wi-Fi enabled devices.

Wireless local area networks

WLAN is a wireless local area network that, as mentioned above, links two or more computers or devices using spread spectrum or OFDM modulation technology, in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

Wireless LAN technology was developed as early as 1991 when wireless LAN products had just appeared in the market and the IEEE 802.11 committee was just standardising the protocols. In less than five years, the technology gained widespread application and implementation, with hospitals, colleges and stock exchanges all being enabled for nomadic access, point-to-point local area network bridges, ad-hoc networking and internet access.

Wi-Fi and wireless LAN have become more accessible and convenient in recent times due to falling equipment prices

We have discussed how all it takes to enable Wi-Fi technology is the small radio. However, initially, the WLAN hardware was so expensive it was used only as an alternative to cabled LAN in places were cabling was difficult or inefficient. However, since the IEEE standards emerged and there was a proper industry focus on interoperability and the growth of the Wi-Fi Alliance, the WLAN has taken great strides in development.

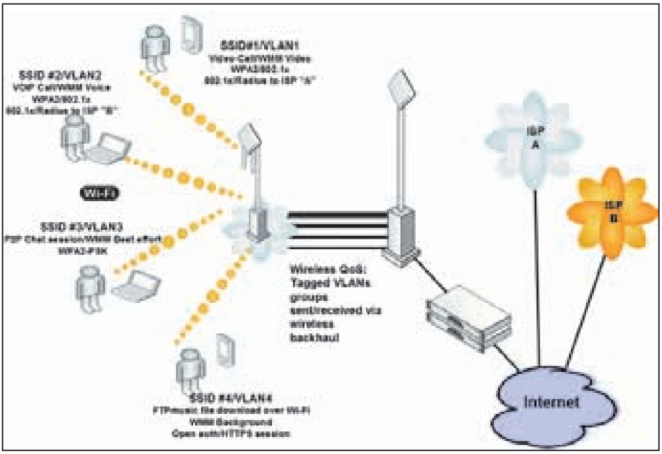
All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface cards (WNICs) which contain the main hardware and embedded protocols for transmission of data across the spectrum.

Wireless stations fall into one of two categories: access points and clients. The basic service set (BSS) is a set of all stations that can communicate with each other. The BSS can be understood as two basic types: independent and infrastructure. The independent one is an ad-hoc network that contains no service points. The infrastructure service set communicates with other stations, which though not in the same basic service set, are linked by access points.

An extended service set (ESS) is a set of inter-connected Basic Service Sets (BSSes). Access points in an ESS are connected by a distribution system. A distribution system connects access points across an ESS. Each BSS has an ID called the BSSID which is the MAC ID of the access point and each ESS has an ID called the SSID which is a 32-byte (maximum) character string. Both together allow for identification.

Peer-to-peer: an ad hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one device gives permission to talk. This is accomplished using the independent basic service set (IBSS). A peer to peer network allows wireless devices to communicate directly with each other. Once two devices are within range of the other, they can communicate independently without any central access points. Once they interact with each other, this initiates the formation of a network.

If a signal strength meter is used in this situation, it may



An example of a network with various devices performing various tasks not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may simply be the closest computer. The IEEE 802.11 specification includes provisions designed to minimise collisions between two independent transmissions. Two mobile units may both be in range of a common access point, but not in range of each other. Therefore, the 802.11 standard has two basic modes of operation: ad hoc mode enables peer-to-peer transmission between mobile units, and using the infrastructure mode, mobile units communicate through an access point that serves as a bridge to a wired network infrastructure. Since wireless communications use a more open medium for communication in comparison to wired LANs, the 802.11 designers also included shared-key encryption mechanisms. Some examples are the Wired Equivalent Privacy (WEP) and the Wi-Fi Protected Access (WPA, WPA2) which are used to ensure security.

Bridge: a bridge can be used to connect different networks. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN. This way, any device within range of another device with an internet connection can access the internet.

Roaming is not limited to cellular networks. Even wireless LANs encounter roaming

Wireless distribution system: a wireless distribution system allows the wireless interconnection of access points in an IEEE 802.11 network. If a proper distribution network is set up, then a wireless network can be expanded using multiple access points without the need for a wired backbone system to link them. The advantage of a distribution system is that it preserves the MAC addresses of clients.

Roaming: in a wireless local area network, there are two types of roaming. Internal roaming occurs when the mobile station moves from one access point to another within, say, a home network. If the network signal is too weak and connectivity is not maintained during the switch from one access point to another, the data transfer will be interrupted. Hence, there are software solutions to maintain connections.

Also, the mobile station is continuously on the alert for alternative access points. The software solutions provide for session persistence. External roaming occurs when a mobile station moves into a WLAN of another wireless internet service provider (WISP) and takes their service. For using the wireless service provided by a foreign network (which is not the user's home network), it has to be open for visitors and there will be special authentication and billing systems for such mobile services.

Hotspots

a hotspot is a physical location that offers internet access over a wireless LAN through the use of a shared internet connection and a single router. There are many hotspot locations available in the west, but in India, the concept is yet to take off. However, there are several academic institutions that have WLAN enabled and serve as a hotspot. Anyone can use a laptop or a Wi-Fi phone or any other portable device to access Wi-Fi. There are several locations which have broadband enabled internet access. Procuring a wireless router, interfacing it and getting access to the internet then becomes simple.

The next time you sit in a coffee shop, check if it has a free hotspot

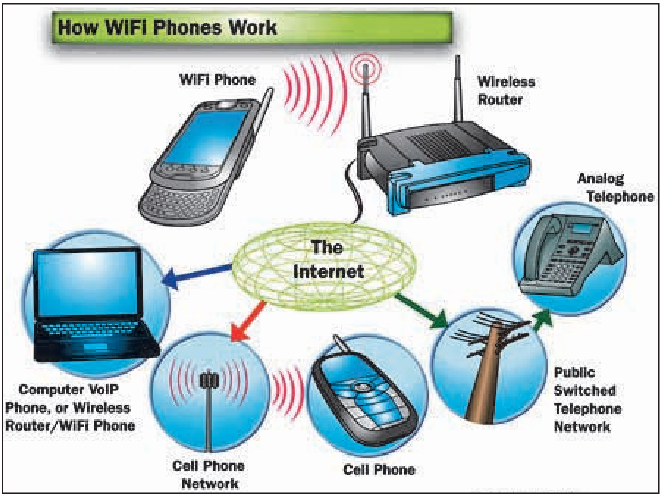
Free hotspots operate in two ways. One is to use the open public network. One Wi-Fi router and then private users of wireless routers can turn off their authentication, thus opening their connection, allowing anyone in range to share. Certain closed public networks use a hotspot management system to control and allow only specific users to access the internet, or maybe restrict individual downloading capability or charge per minute for downloaded information. Bandwidth restriction is also possible. A specific type of closed public network is a commercial hotspot. For certain places where authentication and/or payment is required, there are proper authentication, user level access enabled systems. Software solutions are also available for this. Though some restaurants, lounges, airports provide Wi-Fi access as part of customer service, you are likely to be charged for using the internet in other places.

In the early 2000s, when Wi-Fi usage was starting to boom, several cities anticipated a city-wide WLAN in place. This is often referred to as a municipal wireless network. However, the task seemed to be of quite some magnitude and not all projects succeeded. In 2005, Sunnyvale in California became the first city in the USA to offer city wide free Wi-Fi. If such a service were to be enabled in every city, this would unleash enormous potential for information sharing, public news service, broadcasting announcements, mobile commerce and so on.

6.3 Features of Wi-Fi, advantages and disadvantages of Wi-Fi

The advantages of a Wi-Fi network are several. The most obvious one to begin with is that it is wireless. This allows local area networks to be initiated without wires for client devices. Wireless LAN's have great potential for expansion in several space-constrained regions. Nowadays, wireless network adapters are built into most laptops. With the prices of the chipsets steadily reducing over the years, Wi-Fi has developed into an economical networking option, especially for corporate infrastructures.

Also, since the Wi-Fi certified brand by the Wi-Fi Alliance



Many devices, one connection – Wi-Fi phone allows for backward compatibility and interoperability, Wi-Fi has become very widespread and prolific in terms of the number of users and geographic capture of markets. A standard Wi-Fi device should actually work anywhere in the world as the core concept is the same, although the spectrum assignments and operation limitations are not consistent internationally.

However, most Wi-Fi networks have a limited range. A typical router at home with Wi-Fi capabilities might barely extend more than 300 feet outdoors. However, the newest IEEE standards (the ones developed after 802.11b or 802.11g) have better ranges. Wi-Fi in the 2.4 GHz spectrum has a slightly better range than the 5.0 GHz frequency block. However, depending on the antenna, the outdoor range of Wi-Fi can be improved and extended up to several kilometres.

Long range Wi-Fi is one of the most recent developments with people envisioning Wi-Fi as an alternative to satellite coverage. However, these devices are in the early stages, and have neither been certified as Wi-Fi products nor have they been certified for interoperability.

Wi-Fi security is of prime concern, especially in days of terrorist and cyber attacks

Depending on usage, range and other specifications, the power consumption varies. However, given its range and utility, the power consumption is much higher than with other low range technologies such as Bluetooth. A difficulty therefore arises when using Wi-Fi on mobile phones and other small devices with minimal battery life.

The complex nature of radio propagation at typical Wi-Fi frequencies makes it difficult to identify specific connection strengths without direct data transfer. A Wi-Fi signal only gives the signal strength for the nearest device. The reflection of these electromagnetic waves across certain media and blockage and interference are other factors that need to be considered.

As Wi-Fi networks have a limited range, jumping from one hotspot to another is a good way to permanently stay connected to the internet. The process of going around looking for Wi-Fi for wireless internet access is called Wardriving.

There are other issues to be considered such as security.

Wi-Fi access points often have their status as “open”. Novice users often initiate the network procedures without realising that other people could be latching onto their computer, thereby gain access to their wireless LAN and browsing the internet for free – or worse, stealing data. The most common wireless encryption standard WEP (Wired Equivalent Publicity) and even the WPA and WPA2 Wi-Fi Protected Access can be broken. Unencrypted devices are certainly at major risk, but so are protected ones. Open networks can also be monitored so user data can be witnessed and copied.

We have also earlier mentioned the extent to which the 2.4 GHz spectrum channel is overcrowded, with so many wireless technologies utilising it. Other technologies using this spectrum include systems such as Bluetooth.

Another term you will come across is Wi-Fi pollution – this is used to describe an excess number of access points in an area, especially on the same channel. This can cause reduced bandwidth, more infrequent connectivity, lower signal-to-noise ratios, and can be a serious problem. In a large apartment / work complex, there could be a large number of Wi-Fi access points, along with parallel crowding of Bluetooth, microwave ovens, security cameras and the like. The general advice for those who suffer from interference is to migrate the Wi-Fi connectivity to the 5 GHz spectrum, parts of which are also unlicensed.

With cheap wireless routers, you don't need cable clutter anymore. Just hook up a wireless network card and get rid of those cables

Workshop: Enabling Wi-Fi on your computer

Now, if you have bought your computer recently, or have a laptop, chances are that you have Wi-Fi access. Microsoft Windows, for example, has comprehensive driver-level support for Wi-Fi, the quality of which depends on the specific hardware manufacturer. Most hardware vendors ship the default Windows drivers along with their products. Earlier versions of Windows, such as 98, ME and 2000 do not have built-in support for Wi-Fi drivers. So, if you possess one of the older versions, you will need to get the software from the manufacturer, most often by downloading from their website. Microsoft Windows XP has built-in options to manage and configure networking. However, support for WPA2 and some other security protocols require updates from Microsoft. XP has a strange way of connecting to the wireless network. In case there is a problem regarding the wrong passphrase for closed networks, it keeps connecting without notification that the passphrase is wrong. There are a few other problems as well. But for the generic user, Windows support is sufficient to connect and work with a Wi-Fi network, although more picky users might be insistent on getting their own driver and software support. Vista has improved Wi-Fi support as does Windows 7 (the release candidate at least).

Getting set up is easy and before long you'll be able to browse wirelessly

Linux, FreeBSD and similar Unix-like clones have support for Wi-Fi though this is not very standardised as the very nature of these platforms is open source. Linux has patchy Wi-Fi support, though native drivers for many chipsets are available at little or no cost. Since open source is not as prolific as it could be, many small hardware manufacturers skip making drivers for Linux.

Let's try setting up a wireless network and connecting to the internet using it. We assume that you neither have the hardware capability nor the drivers installed and so we shall begin from scratch. Users who possess just the first or both may proceed from wherever necessary in case they wish to go through the workshop. This tutorial will serve several purposes: installing a Wi-Fi device, setting up a Wi-Fi network and connecting to the internet via a bridged network. Wi-Fi hotspots work on the same principle.

We shall begin by assuming that you have Windows XP Service Pack 2 installed. Also, that you have or will soon purchase an external device that will allow you to access Wi-Fi. Wi-Fi dongles (small piece of hardware) are available in USB format or using PC slots. You may choose either.

The steps that you need to follow are the following

- Choose your wireless equipment.
- Connect your wireless router.

- Configure your wireless router.
- Connect your computers if there is an existent network or create a new one.

Choose your wireless equipment.

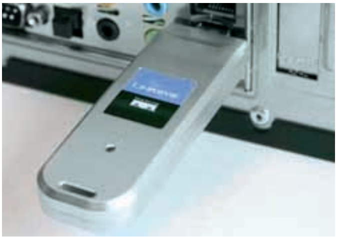
Choosing equipment is essential. As mentioned earlier, there are three different technologies: 802.11a, 802.11b and 802.11g. 802.11g is a safe bet, though if picky, any other should do. Check for range specifications. Also, if there is a likelihood of several devices operating in the spectrum range, choose something else.

Wireless Router

What you should have or what you need:

- Internet connection (only to create a network to access the net – for a small wireless area network, you do not need internet access).
- Wireless router.
- A computer with built-in wireless networking support or a wireless network adapter.

The router converts the signals coming across your internet connection into a wireless broadcast. A router is essential. Network adapters wirelessly connect your computer to your wireless router. You might not need this in case it is a newer computer. In case of a desktop, we recommend a USB wireless network adapter. In case of a laptop, a PC card-based one should do the trick. Make sure that you have one adapter for every computer on your network.


Wi-fi USB stick

To make setup slightly easier, choose a network adapter made by the same vendor that made the router.

There are several available in the market today. Even Microsoft sells both. Of course, it is assumed that you have USB / PC-card slots free.

Connect your wireless router

First, find your cable or DSL modem and switch it off. Then, connect your wireless router to your modem. Ensure that your modem is connected directly to the internet. Later, after you've hooked everything up, your computer will wirelessly connect to the router, and the router will send communications through your modem to the internet.

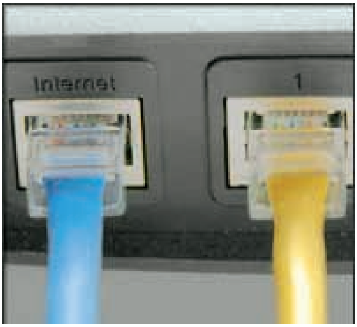
If your computer is connected directly to your modem, then unplug the network cable from the back of your computer, and plug it into the port labelled internet, WAN, or WLAN on the back of your router.

If you do not currently have a computer connected to the internet: plug one end of a network cable (included with your router) into your modem, and plug the other end of the network cable into the internet, WAN, or WLAN port on your wireless router.

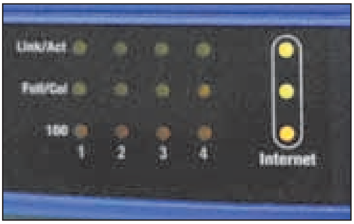
In case you already have a router, replace it with this one and follow the above instructions.

Ensure basically that your modem is connected to your wireless router. And that the modem is connected via cable to the port labelled internet on the back of your wireless router.

Next, plug in and turn on your cable or DSL modem. Wait a few minutes to give it time to connect to the internet, and then plug in and turn on your wireless



Wireless Router – connect to internet port



Modem lights come on

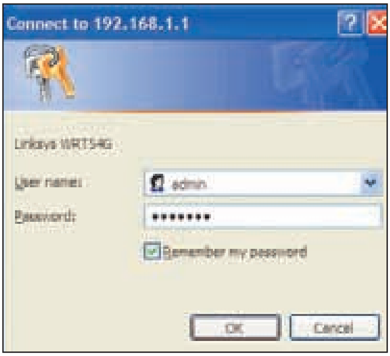
router. After a minute, the internet, WAN, or WLAN light on your wireless router should light up, indicating that it has successfully connected to your modem.

Configure your wireless router

Using the network cable that came with your wireless router, you should temporarily connect your computer to one of the open network ports on your wireless router (any port that isn't labelled internet, WAN, or WLAN). If you need to, turn your computer on. It should automatically connect to your router.

Next, open Internet Explorer and type in the address to configure your router. The address and other similar details should be given in the user's manual of the router.

You might be prompted for a password. The address and password you use will vary depending on what type of router you have, so refer to the instructions included with your router.



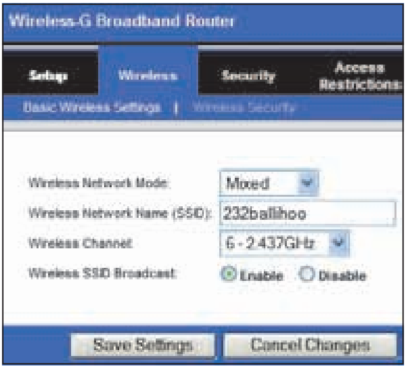
Linksys WRT54G

User name: admin

Password: ••••••••

☑ Remember my password

Entering the username and password



Wireless Network Mode: Mixed

Wireless Network Name (SSID): 232ballihoo

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ● Enable ○ Disable

Naming the network

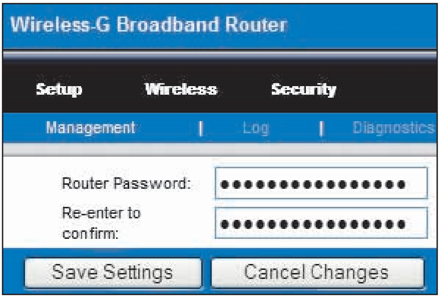
Internet Explorer will show your router's configuration page. Most of the default settings should be fine, but you should configure three things:

- Your wireless network name, known as the SSID. This name identifies your network. You should choose something unique that none of your neighbours will be using.
- Wireless

encryption (WEP) or Wi-Fi protected access (WPA), which help protect your wireless network. For most routers, you will provide a passphrase that your router uses to generate several keys. Make sure your passphrase is unique and long.

- Your administrative password, which controls your wireless network. Just like any other password, it should not be a word that you can find in the dictionary, and it should be a combination of letters, numbers, and symbols. Be sure you can remember this password, because you'll need it if you ever have to change your router's settings.

The exact steps you follow to configure these settings will vary depending on the type of router you have. After each configuration setting, be sure to click Save Settings, Apply, or OK to save your changes.


Wireless-G Broadband Router

Router Password: ••••••••••••••••

Re-enter to confirm: ••••••••••••••••

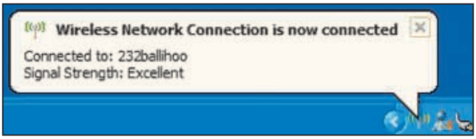
Setting an administrative password

Now, you should disconnect the network cable from your computer.

Connect your computers

If your computer does not have wireless network support built in, plug your network adapter into your USB port in the case of a PC, or insert the network adapter into an empty PC card slot, in the case of a laptop. Windows XP will automatically detect the new adapter, and may prompt you to insert the CD that came with it. Usually, there is native support for several of these. But in the rare case that there isn't, ensure that the CD that came along is at hand. The on-screen instructions will guide you through the configuration process. Clicking next and agreeing to the terms and conditions, if any, should do the trick.

Windows XP should show an icon on the taskbar with a notification that says it has found a wireless network. In case it cannot detect any wireless network, it will let you know this.



Wireless Network Connection is now connected

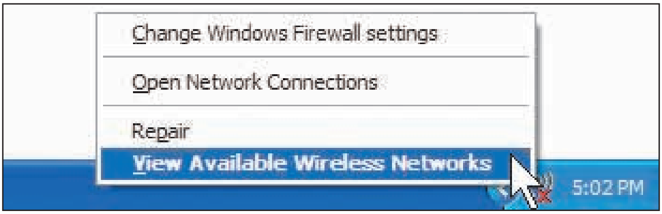
Connected to: 232ballihoo
Signal Strength: Excellent

The pop-up alerts you of your connection status

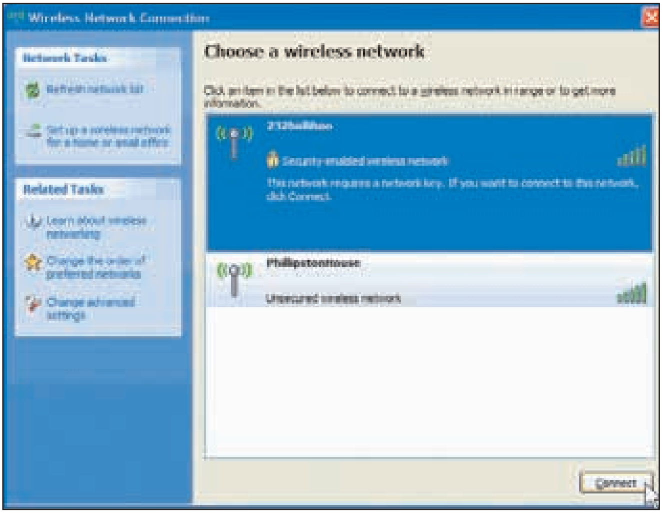
If that is the case, check if the above instructions have been followed, and if all the connections between the router and modem are tight.

Follow these steps to connect your computer to your wireless network:

- Right-click the wireless network icon in the lower-right corner of your screen, and then click View Available Wireless Networks.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks
5:02 PM

View available networks


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

212ballihoo

Security-enabled wireless network

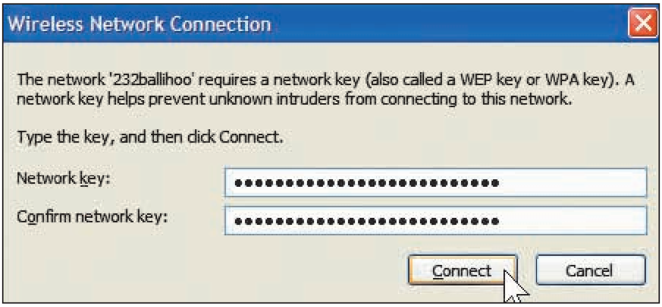
This network requires a network key. If you want to connect to this network, click Connect.

Phillipstonhouse

Unsecured wireless network

Connection to a Wi-Fi network is a matter of clicks

- The Wireless Network Connection window should appear and you should see your wireless network listed with the network name you chose. If you don't see your network, click Refresh Network List in the upper-left corner. Click your network, and then click Connect in the lower-right corner
- Choose wireless connection
- Windows XP prompts you to enter a key. Type the encryption key that you wrote down earlier in both the Network key and Confirm network key boxes, and then click Connect.
- Windows XP will show its progress as it connects to your network. After you're connected, you can now close the Wireless Network Connection window. You're done.



The network '232ballihoo' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●●●●●●●●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●●●●●●●●●●●●●●●●

Type encryption key for access.

Note: If the Wireless Network Connection window continues to show Acquiring Network Address, you may have mistyped the encryption key.

You can now wirelessly access your internet from anywhere in the room, with your modem somewhere else. Having done this, you can now try it out at a Wi-Fi hotspot. Spotting hotspots is easily done. There are several websites on the internet that list them. Alternatively, there are programs like NetStumbler available which help you locate Wi-Fi hotspots nearby in case you are travelling.

6.4 The future of Wi-Fi

Much like Bluetooth, Wi-Fi offers wireless connectivity, but with a difference. The primary point is that though it consumes more power than other short range technologies, it has options such as accessing free internet through hotspots. Ask anyone the easiest way of connecting to the internet using a laptop, and the answer would most likely be Wi-Fi. The term itself has become so synonymous with Wireless LAN, it's obvious that the brand has made a good image and reputation for itself.

With better specifications coming out and Bluetooth also jumping onto the 802.11 protocol, Wi-Fi is obviously here to stay. Also, developments over the years have reduced the cost of WLAN hardware greatly.

In several cities in the USA, almost all of their technology is wireless, with internet accessible via mobile and laptop. The scope for a municipal wireless network is there and the potential is huge. A city-wide network would facilitate better data sharing, better information broadcasting, better public systems and better internet on the go. We in India have realised the value of e-Governance. But cities such as San Francisco have initiated systems so that a person can report, say, small city problems such as open drains on a real time platform (Twitter). Any real time work or internet-on-the-go is possible only with the help of wireless local area networks. A Wi-Fi enabled system can do most of the things any other wireless technology can do, but the focus is on speed and widespread easy-to-access connectivity. And Wi-Fi has clearly proved its place.

Short range point to point communication

So far, we have discussed some of the more common applications of wireless technologies. Other examples of wireless technology include GPS units, wireless computer mice, keyboards and headsets.

The term short range point-to-point communication refers to a sub-category of wireless communication. This term can best be understood in reference to the two phrases it contains. The term point-to-point means that the transfer of data takes place directly between the two devices in question. There is no formatting of the data packets involved, and all the responsibilities of completing the data transfer are taken by the devices themselves, and there is no external agency involved. Point-to-point is commonly known as P2P or PtP. The modern definition of wireless point to point communication entails the use of a multi-giga Hertz range of radio signals for wireless data transfer. The term short range is a vague term. There is no international specification as to what constitutes short range wireless communication, but it is usually accepted to be something that is within either visibility range or within audible range.

The field of short range point-to-point communication has now grown and it encompasses a large range of technologies. It has totally revolutionised the process of data sharing as the absence of wires makes is much easier and much less cumbersome than conventional methods of data transfer. Nowadays, with the improvement in radio wave technologies and modulation-demodulation methods, it is now possible to achieve very high speeds of data transfer. These short range methods have transformed our lives. Everywhere we go, we see instances of these technologies being used to facilitate processes. Short range point to point technologies are

We come across point-to-point wireless communication everyday in the form of wireless keyboard and mice many in number. These include remote controls, infrared data transfer devices, radio identification devices and some others. There now follows a brief description of these technologies.

7.1 Remote control

A remote control is a small device that is used to control another device from a distance. Remote controls are now standard accompaniments to various household devices such as televisions, stereo systems and air conditioners. Today, remote controls are usually small, easy-to-handle, handheld devices that possess many buttons which help control the functions performed by these household devices. In fact, nowadays, the remote control is the primary control and it contains all the function controls. The device that is being controlled, on the other hand, usually has only a handful of rudimentary controls on it.

The remote control traces its history as far back as 1898, when Nikola Tesla patented a device, named 'Method of an Apparatus for Controlling Mechanism of Moving Vehicle or Vehicles'. In 1903, Leonardo Torres Quevedo invented a device called the Telekino. The telekino was essentially a robot. This robot executed commands that were given to it by the means of electromagnetic waves. The first remote controlled airplane flew in 1932. As a result of this technology, remote control technology was extensively employed in the Second World War. The first remote control for televisions, called "Lazy bones", was developed by Zenith Radio Corporation in 1950. The impetus to make remotes that would perform several functions began in the late 1970s due to BBC's development of the Ceefax teletext service.

Today, most of the remote controls available are consumer

11 different remote controls kept side by side

IR devices that communicate with the controlled peripherals using infrared. A handful of remote controls also use radio signals. However, this has not proved popular, mainly because early radio TV remote controls would often switch channels on a neighbour's TV as well as on their owner's. As it does not pass through walls, most remote controls for electronic devices use an infrared diode. This diode emits a beam of light, typically with a wavelength of 940 nm. This beam of light reaches the device receptor and thereby controls it. This emitted beam of light is invisible to the human eye but not to video cameras, which see the diode as if it produces a purple light.

The presence of a carrier signal is used to trigger a function in the case of a single channel remote (single-function, one-button). There are many procedures that may be used in multi-function remotes. One of these consists in using signals of different frequency to modulate the carrier signal. The appropriate frequency filters are then applied to separate the signals after the demodulation of the received signal. However, these analogue methods are fast being replaced by their digital counterparts.

Thanks to the remote, you don't have to walk each time you want to switch channels on the television

An AM radio in very close proximity to a remote being operated is often an excellent means of hearing the signals being modulated on the infrared carrier.

In order to distinguish between the controls of devices from various companies, each company uses a different protocol to transmit infrared commands. Some of the different protocols that are employed are the different SIRCS versions used by Sony, the RC-6 from Philips, or the NEC TC101 protocol.

Remote controls are now extensively used in many areas including the military, space, industry, toys and video games.

There is no doubt that remote controls have transformed our lives and have greatly simplified the use and control of various household gadgets. However, there is a great increase in the number of gadgets in the average household and thus there is a related increase in the average number of remotes per household. A home may have up to eight different remotes at any given point of time and thus the use and operation of all these gadgets simultaneously becomes extremely cumbersome. Due to this universal remote controls, which can control a number of devices at the same time, are becoming increasingly popular. A universal remote control is a device that can send different carrier signals which are programmed so that they mimic the signals sent out by many electronic gadgets. As a result of this, a single remote can be used to control many devices at a time.

7.2. IrDA

IrDA stands for InfraRed Data Association. It defines the standards related to the transfer of data between two devices using infrared light.

The IrDA defines standards related to the transfer of data between two devices using infrared

Infrared communication is a form of free space optical data communication.

For the devices to communicate with each other, they need to have a direct line of sight. Thus, infrared communication comes under the category of very-short-range communication. There are many kinds of IRDA specifications. These include IrPHY, IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, IrLAN and IrSimple. These specifications are arranged from the lowest layer to the highest layer. This means that for IrLAP to be possible, IrPHY must be present, and so on. Here is a brief description of each of these specifications:

IrPHY (Infrared Physical Layer Specification)

This is the lowest layer of specifications and facilitates speeds between 2.4 kbit/s to 16 Mbit/s. The wavelength of light used lies at 875 +/- 30nm. IrPHY usually operates in a cone with a semi-angle of 15 degrees. Most IrPHY devices ideally operate in the distance range of 5 to 60 cm apart. These need to have a certain minimum irradiance in order to be visible, while at the same time, not being blinding to the other device when brought close. While transmitting, a device's receiver is usually blinded by its own light and thus, it is possible for only one direction of data travel at a time. The data transfer rates are divided into Serial Infrared (SIR), Medium Infrared (MIR) and Fast Infrared (FIR). All transfer and discovery is performed at a baud rate of 9,600 bits/second because this is the least common denominator of data transfer speeds.

IRLAP (Infrared Link Access Protocol)

This is the second layer. In this specification, the devices are divided into primary devices and secondary devices. The secondary devices are controlled by the primary devices, and only upon request from the primary device can they send data. This consists in granting access control and establishing an efficient bidirectional data communication system. Once the communication partners are established, the primary device and secondary device roles are distributed.

IrLMP (Infrared Link Management Protocol)

This is the third layer of IrDA specifications. It consists of two parts, the LM-MUX (Link Management Multiplexer) and the LM-IAS (Link Management Information Access Service). The LM_MUX provides multiple logical channels and provides the ability to change the primary and secondary devices. The LM-IAS provides a list, where service providers can register their services. Thus, these services can be accessed by querying the LM_IAS.

Infrared connectivity is used in basic applications such as TV remotes to wireless LAN connectivity

Tiny TP (Tiny Transport Protocol)

This is an optional specification that makes use of SAR (Segmentation and Reassembly) in order to transport large messages. It also makes use of every logical channel and thus provides control of data flow.

IrCOMM (Infrared Communications Protocol)

This is once again an optional specification. It enables the infrared device to act like a port, which may be either serial or parallel.

IrOBEX (Infrared Object Exchange)

This is yet another optional specification that facilitates the exchange of arbitrary data objects between infrared devices. Tiny TP is a necessity in order for IrOBEX to work. Complex data structures like applications and even calenders can be exchanged with this.

IrLAN (Infrared Local Area Network)

This is an optional specification and facilitates the connection of an infrared device into a Local Area Network. Once again based on the Tiny TP specification, it accesses the LAN by one of three methods. These are Access Point, Peer-to-Peer (P2P) and Hosted.

IrSimple

This specification works by improving the efficiency of the IrDA protocol. As a result of this, you can get speeds at least 5-10 times faster than with the standard protocol. As a result, it is possible to transfer a picture from a cell phone within about one second.

IrSimpleShot (IrSS)

This is a revolutionary specification whose primary purpose is the facilitation of picture transfer from IrDA enabled camera phones to printers, printer kiosks and flat panel televisions.

IRDA via USB

7.3. RFID

RFID is a process by which an identification device is incorporated into an object or even a living being i.e. a human or an animal, for the purpose of identification. If used correctly, RFID can be the quickest and simplest method of identification as it is completely unobtrusive, and the inherent need for digital technology makes it much faster than any identification process which is overseen by humans.

An RFID tag used for electronic toll collection

The predecessor of RFID technology is considered to be a device that was invented in 1946 by Leon Theremin as an espionage tool for the Soviet Union. This was, in fact a covert listening device that transmitted radio waves with audio information.

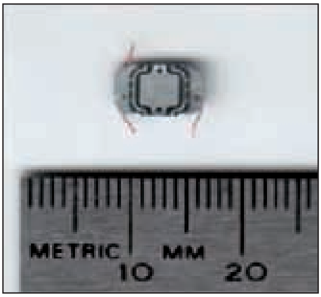
The era of RFID can be first solidly traced back to a patent in 1973 by Mario Cardullo. This consisted of a passive transponder with memory. The device is passive but it can be made active by means of an interrogating signal. Cardullo himself foresaw the uses to which this new technology would be put, and he demonstrated it in 1971 to the New York Port Authority and other potential costumers as a means to collect tolls. The name RFID was first used in a patent that was granted in 1983 to Charles Walton.

An RFID device essentially consists of two parts: an integrated circuit and a receiving device. The integrated circuit consists of circuitry that stores the required information and also modulates and demodulates the RF (radio frequency) waves. The receiving device on the other hand receives and transmits the required signals.

The simplest example of an RFID system is the access cards used by companies to govern employee movement

RFID tags can be divided into three main groups: active, passive and battery assisted power (BAP). Active tags can transmit signals by themselves as they contain batteries. Passive tags, on the other hand, can transmit signals only in the presence of an external source. BAPs require an external source to transmit, but they also contain a battery and thus their signals are strong, providing great range.

The reason that RFID is so successful is the fact that the devices can be made really small. This makes them unobtrusive and easy to incorporate into pretty much anything. The smallest radio transponder in the world is the Hitachi μ-chip (or mu-chip). It measures only 0.4 mm by 0.4 mm – rather



PayPass RFID chip removed from a MasterCard

like a small grain of sand. Despite its size, the mu-chips are provided with 128 bits of ROM and this enables them to store 38-digit numbers. In fact, earlier this year, researchers at the Bristol University managed to successfully glue micro-transponders onto a colony of live ants. This helped them study their behaviour and consequently understand ant-hill dynamics. The only problem with having such small chips is that the ability to read is constrained by the inverse-square law. Thus to give it a large range, the signal strength will need to be made quite high.

RFID tags are also becoming extremely cheap, and this further makes them a viable resource. In fact, earlier this year, Envego released a tag that costs only 5.9 cents a tag (Rs. 2.50 a tag).

The largest employer of RFID tags in the world is the USDOD (United States Department of Defence). They use RFID tags to tag every single container that goes out of the continental United States (CONUS).

There are however, quite a few controversies involving RFID. There are many organisations that have raised privacy issues.

RFID systems have been accused of invading employee privacy

The chief concern for many is the fact that, at times, people may not be aware that they have been tagged. Also, a world-readable tag can make them prime prey to malicious intent. Another concern is that often the things people buy may be radio tagged. The size of the tag makes it impossible to detect, and thus these items may be used to carry out surveillance on the unsuspecting victim. It is also possible to program machines that read the identity from the tags, thus severely compromising security. Another, more technical, fear is that it is unknown what repeated exposure to radio waves can do to a person's physiology. There is no doubt that RFID has revolutionised lives all over the world, but, it is true, that it also has some fears associated with it, which will need to be allayed.

7.4 Wireless sensor network

A wireless sensor network (WSN) is a set of autonomous machines that use in-built sensors to cooperate, and together monitor physical phenomena such as sound, temperature, pressure, etc. Like all networks, a WSN also consists of individual components called nodes. In a WSN, each node contains the required sensor, a microcontroller, a battery and a communications device such as a radio transceiver.

Wireless sensor networks were initially built as a military tool and used as a surveillance mechanism

Apart from the nodes, there needs to be a control unit in the WSN. This unit is in charge of processing all the data that is gathered by the various sensors which are in operation. It is also usually programmed to analyse the data gathered and thus reconstruct the required phenomenon.

Some of the characteristics of the WSN make it unique. Nodes in the WSN are built for specific conditions and thus can withstand extremes in environmental conditions. In a WSN, the failure of one node does not lead to the failure of the system. The rest of the nodes will continue to function and will all do their job. Another unique aspect is the dynamic network topology. Being wireless, the nodes can be shifted anywhere and they can also keep exchanging roles without a problem. This is an advantage when something is being monitored that changes rapidly. The biggest advantage is that the operation of a WSN does not need to be constantly monitored, and this makes it suitable for use in conditions where human interference is not possible.

However, there are also some problems with a WSN system. The biggest is that the power source that a node uses is a battery. This makes the node functionality limited to the battery life. There is also higher risk of communication failures because of the environment, and these are also harder to repair.

The battery constraints make it necessary that the programs in use in the system are all fast, efficient and focussed. The algorithms need to be robust and self configuring. The operating systems that are used also need to be streamlined because they are made for a specific purpose. As a result, the operating systems used in WSN systems are much less complex than the usual ones in PC systems. The system is similar embedded systems and thus it is also possible to use the OSs that have been developed for those purposes.

WSN was initially developed as a military tool and was used as a surveillance mechanism. Nowadays, however, there is widespread use of WSN in various areas such as health care, environment monitoring, global warming, area monitoring, wastewater monitoring, etc. There are also simulators that help in modelling and creating Wireless Service Networks.

7.5 Miscellaneous short range communication

There are many applications that the various short range point-to-point communication systems have been put to. These include many things that have revolutionised aspects of our lives. Some of these are:

- The National Database and Registration authority (NADRA) in Pakistan and also the Transport department of New Delhi have issued driver's licences that have RFID tags on them. There is a database that stores the information of all the licence holders. The database also contains a history of all past offences that a driver has carried out, which includes data regarding traffic violations, tickets issued, and outstanding penalties. The traffic police are supposed to carry identification machines that can help gather information from the RFID tags in the licences. This helps greatly speed up the process of prosecution of driving offences. It is even possible to cancel the driving licence electronically in case the concerned person carries out some serious offence.

RFID tags are being used by transport authorities to keep track of the offences committed by drivers

- Some theme parks around that world provide their customers with wristbands that contain an RFID tag. This helps the park to identify the various costumers and where they are at any given point of time within the park. This also helps them make a customised DVD of the time spent by each customer at the park at the end of the day. These DVDs are available for sale at the end of each day.

- The Attorney General's office in Mexico has been using an RFID tag called the verichip since 2004. According to that initiative, in order to control access to a secure data room, 18 of the members of the office were implanted with the verichip. This thus helps identify the location of each of the members within the facility at all times.
- One of the main uses of RFID tags is in libraries where the intention is that this technology will replace barcodes. The identifying information of the items in question can be stored in the RFID tags. The information is then read out by the RFID reader which performs the same function as a barcode reader. It does not need to make use of a separate database in order to access the information such as the book's title or its material type. It can be used to augment the usage of barcode readers by offering a means of inventory management. It can also replace the barcode readers and make the whole process one of self service for the borrowers. In some places, membership cards are also provided with RFID tags.

Delhi Metro uses RFID smart cards as part of its ticketing system. These cards are programmable at kiosks

- Recently, the Delhi Metro Rail Corporation (DMRC) has started issuing smart cards to its patrons. This is a card that can be reprogrammed in a kiosk. The customer pays some money and that much money is added to the contents of the card. A person can travel without purchasing tickets for as long as he/she has money left in the card. It uses RFID tagging to store the information. Every time a person uses the metro, the required money is debited. A person merely needs to place their card in a slot, a radio wave reader in it processes it and the transaction is carried out automatically.
- Some casinos are using RFID tags in the gambling chips that they provide. This helps to track the location of the chips on the casino floor. This in turn can help to identify counterfeit chips and to prevent the theft of chips.

Workshops

RFID tagging your valuables:

Isn’t it a real pain to keep sight of all the valuables that you possess? Not only the obvious things like jewellery, but car keys, credit cards, ATM cards and all those things that you cannot just put away in a safe, because you need them for your day-to-day life. Wouldn’t it be nice if there was a way to monitor all of your personal belongings just sitting at one place? Well, nowadays, there are many kits available that can enable you to do just that.

One of them is an RFID kit called RFID Toys, that is manufactured by Trossen Robotics. This experimentation kit contains over a dozen types of RFID tags, a USB based RFID reader and instructions for tons of insidious RFID projects. You even get a cool bio-implantable type of RFID tag. All you need to do is to install a program. Plug in the USB reader, put in the tags, and you are good to go.

While it's relatively easy to get the software installed and the USB RFID reader recognizing tags, it is hard to carry out any advanced applications. But, this system gets you accustomed to the nitty-gritties of RFID tagging while sitting in your own home.

Kit Contents:

- Phidget USB RFID Reader
- USB Cable
- RFID Toys Book Covering RFID Projects and Downloadable Software
- One Blue Aquatic Key Chain
- One Credit Card Thin Card
- One Clamshell (thick) Card
- One Small Glass Ampoule

A home RFID tagging system

- One 17 mm Black Pill Tag
- One 30 mm Global Disc Tag
- One 35 mm White Disc with Hole
- One 50 mm Button with Sticker Backing
- One 20 mm Button with Sticker Backing
- One Inventory Label - Square Version
- One CD-ROM Tag
- One 30 mm Clear Thin Lamination Disc
- One 25 mm Clear Thin Lamination Disc
- One 30 mm Clear Thin Lamination Disc with Sticker Backing
- One 25 mm White Disc

Note: Tags May Vary Slightly from the Assortment Listed

These tags can be used to tag pretty much every conceivable kind of valuable that one may possess. You then install the software and monitor the items from your own personal computer. As long as you have a free USB port, you can use this RFID system thanks to the USB RFID reader.

USB RFID Reader Specifications

This reader can read the RFID tags up to a range of 4 inches depending on the tag used. However, if one wants to increase the range, for security or doorway systems or any other purpose, there is a +5V output so that you can power an external relay source. There is an onboard green LED which can help you check whether there is anything being detected or not. You can also turn off the RFID as and when you want.

Using a universal remote control to control all AV devices at once

Is it not so much of a hassle to actually individually control every audio-visual device that you possess? Does it not irritate you to hunt for, and then continuously fiddle with the remotes of your television, DVD player, set top box and your music system? Here is the solution to those problems. Using a universal remote control for this purpose provides a very efficient alternative. One such available remote control is the Energy Saver Universal Remote Control Kit.

One of the best features that this possesses is that it can completely switch off all the programmed AV devices at the press of a single button. It also has the capability to wirelessly upgrade any new device code, which makes it extremely trustworthy and immune to changes in technology. This remote can be used to control up to four AV devices at a time and is expandable with power plugs. You can also issue multiple commands by pressing a key called the macro key. It also has a learning function which can be used to program any special feature of any remote control into it; this means that this one remote can perform every single function that four others together could.

A universal remote control

Some specialised wireless applications

The applications of wireless technologies that we have seen so far are limited to a specific region or to the transfer of small amounts of data without the use of wires. However, the applications that we are about to see now transcend all such petty boundaries. From a wireless system that spans the whole globe to a system that can actually power our appliances and devices without the use of wires, the forthcoming technologies truly boggle the mind.

First we have the global positioning system (GPS); this is a navigational system that has transformed the very meaning of the term. It can be used anywhere in the world and can help you pinpoint your location on the globe at any given point of time. The other is a fledgling technology which involves wireless power transfer. Although still in its initial stages, the technology has been quite encouraging so far and the day is not very far off when wires will become a thing of the past and we will be able to transfer energy by air alone. These are therefore technologies that have the capability to change the very face of civilisation as we know it.

8.1 Global positioning system

The global positioning system (GPS) is widely regarded as one of the most important inventions of the current era. It provides civilians with the capability to find out their exact location on the Earth from anywhere. It can also help in finding out distances covered in a specified time, rate of descent or ascent, and determining paths to specified locations.

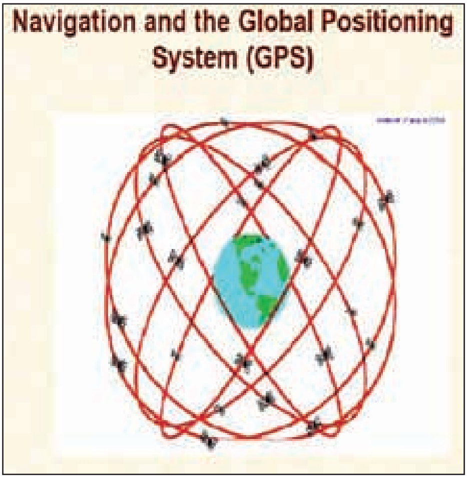
The global positioning system traces its roots back to a navigation system called Transit. First successfully tested in 1960, it was used by the United States Navy. A very basic system, it involved just five satellites. Using these satellites, it could provide a satellite fix approximately once every hour. A major breakthrough in the history of GPS came in 1967, when the US navy developed the Timation satellite. The importance of this was that it allowed for the placing of accurate clocks in space, a technology that GPS heavily relies on.

GPS was developed as NAVSTAR (navigation system with timing and ranging). Before its civilian applications, GPS was used to provide all-weather round-the-clock navigation capabilities for military ground, sea and air forces.

GPS now has applications beyond navigation and location determination. GPS can be used for geography, forestry, mineral exploration, wildlife habitation management, monitoring the movement of people and things and bringing precise timing to the world. It was recently used to re-measure the height of Mt Everest.

GPS satellites continuously transmit digital radio signals that contain data on the satellites' location and the exact time to earth-bound receivers. The satellites are equipped with atomic clocks that are accurate to within one-billionth of a second. Based on the information received, the receivers calculate how long it takes for the signal to reach them, and thus how far away each satellite is.

Initially, the GPS system was intended only for military uses and GPS signals available to civilians were initially distorted. This gave errors of up to 100 metres at times. The resulting average error due to this was 10 metres (32 ft) horizontally and 30 metres (98 ft) vertically. This process of distorting the accuracy of civilian GPS signals was called selective availability. Selective availability was intended to deny an enemy the use of civilian



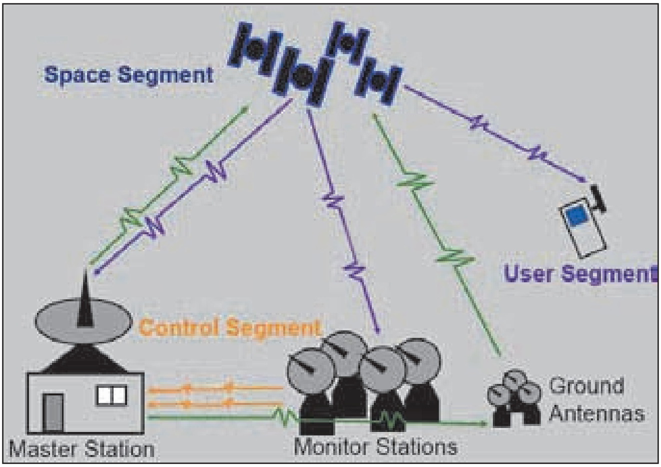
A diagram of the satellites in the GPS system

GPS receivers for precision weapon guidance. However, in 1983, Korean Air Lines Flight 007 was shot down for entering forbidden USSR airspace. This prompted then United States president Ronald Reagan to issue a directive that dictated that civilians would be allowed to use the GPS technology freely. Selective availability was ended in 2000, improving the precision of civilian GPS from about 100 m to about 20 m.

The GPS system originally consisted of 27 satellites that were launched between 1989 and 1993. Out of these 24 were fully functional while the rest are used only for storage purposes. However, as of March 2008, there were 31 active satellites, which further improves the usability and the accuracy of GPS.

The entire GPS system consists of three parts – the space segment (SS), control segment (CS) and the user segment (US). The SS consists of all the satellites that orbit the Earth as mentioned above. The trajectories of the satellites are such that at any given point in time, at any place, there will be at least four satellites which will be in visibility range with respect to the receivers.

The control segment consists of monitoring stations and a master control station. The monitoring stations are in Hawaii, Kwajalein, Ascension Island, Diego Garcia,



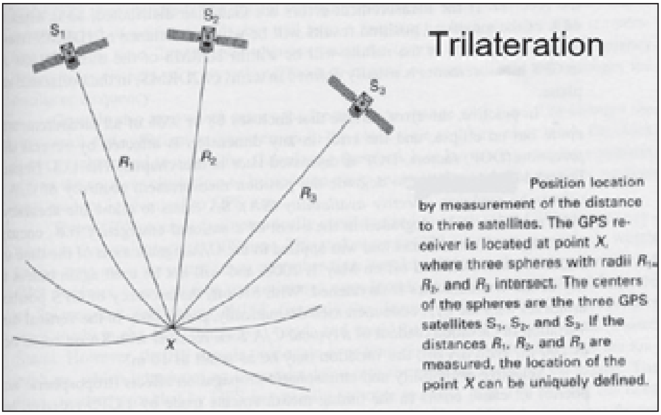
A representation of the segments in the GPS system and Colorado Springs, Colorado, along with monitoring stations operated by the National Geospatial-Intelligence Agency (NGA). The master control station is located at Schriever Air Force Base in Colorado Springs. The tracking information from the monitoring stations is sent to the master control station. The master control station is operated by the 2nd Space Operations Squadron (2 SOPS) of the United States Air Force (USAF). The 2 SOPS use the ground antennas located at Ascension Island, Diego Garcia, Kwajalein, and Colorado Springs to provide a regular navigational update to each GPS satellite. These updates synchronise the atomic clocks on board the satellites to within a few nanoseconds of each other. The inputs from the ground monitoring stations, space weather information, and various other inputs are used by a Kalman Filter to provide the updates.

The user's GPS receiver is the user segment (US) of the GPS. In general, GPS receivers are composed of an antenna, tuned to the frequencies transmitted by the satellites, a clock that is sufficiently accurate so that there is very little error, and a processor that interprets the incoming signals. Some GPS receivers also include a display for providing location and speed information to the user. The number of channels, i.e. the number of satellites it can monitor simultaneously, is often used to describe a GPS receiver. This is a figure that is gradually increasing. Earlier, the number of channels was limited to four or five, but nowadays it is standard for a GPS receiver to have between 12 and 20 channels.

Trilateration is the technique used by GPS receivers to pinpoint the exact location on Earth

In order to pinpoint the exact location anywhere on Earth, the GPS receivers use a technique known as trilateration. In case the receiver receives signals from three satellites, the exact coordinates on the Earth's surface can be provided. However, if there are four satellites, then, the altitude can also be measured. The basic principle of working of trilateration is as follows.

All GPS satellites are time synchronised with each other with the help of caesium atomic clocks. Thus the maximum time error between the satellites is a few nanoseconds. These GPS



Position location by measurement of the distance to three satellites. The GPS receiver is located at point X, where three spheres with radii R_1, R_2, and R_3 intersect. The centers of the spheres are the three GPS satellites S_1, S_2, and S_3. If the distances R_1, R_2, and R_3 are measured, the location of the point X can be uniquely defined.

The GPS receiver calculates its position by analysing the signals from three satellites

satellites each sends out a sphere of signals that all travel with the same speed in all directions (since they are electromagnetic waves, they travel at the speed of light, i.e. around 3,00,000 km per second or 1,86,000 miles per second). It is the intersection of at least three of these spheres that enables the calculation of coordinates. With just three spheres, the object can be at any altitude above the calculated coordinates with respect to the Earth. However, if a fourth satellite is also used, then the exact altitude can also be calculated.

To recap, receivers also have a clock that is synchronised with the satellites, thus, it can calculate the amount of time taken for the signal from each of the satellites to reach it. Thus, using basic distance conversion formulae, it can calculate its exact distance from each of the satellites. Then, using mathematics, and with the prior knowledge of the location of the satellites, it is possible for it to locate the coordinates in a matter of seconds.

However, there are many possible causes of errors, although these are usually minor.

Satellite geometry can affect the quality of GPS signals and accuracy of receiver trilateration.

Dilution of Precision (DOP) reflects each satellite's position relative to the other satellites being accessed by a receiver.

Position Dilution of Precision (PDOP) is the DOP value used most commonly in GPS to determine the quality of a receiver's position.

It is usually up to the GPS receiver to pick satellites which provide the best position triangulation.

Some GPS receivers allow DOP to be manipulated by the user.

Another reason that error occurs is atmospheric effects, the most common being due to the Earth's ionosphere. The ionosphere slows down and deflects electromagnetic signals passing through it. This error is least when the satellite is directly overhead and is greater when it is nearer the horizon, because then the signal has a greater distance to cover through the atmosphere.

Another kind of error is the multipath error. These are due to the reflective properties of radio waves. Sometime the satellite radio waves bounce off objects and are reflected before reaching the receiver. This causes a delay and thus a slight error. However, nowadays, some techniques are deployed to control both of these kinds of errors.

GPS has also recently taken on a new role. This takes the form of satellite navigation in cars and other places and can help a person plan routes and trips in advance. Knowing where the device is in space is one thing, but it is fairly useless information without something to compare it with. Thus, the mapping part of any GPS software is very important; this is how GPS systems works out possible routes, and allows the user to plan trips in advance, and directs the user on the way.

The GPS receiver selects three satellites depending on signal strength to calculate its position

The maps increase the prices of GPS systems. They are loaded into the system and need to be updated quite often. There are, however, several kinds of map, and each is intended for different users, with different needs.

A road user who is planning a trip will only require accurate information about the roads in the region where he is headed. He will not require much information about the terrain of the land, altitudes and other things that a trekker will perhaps require.

On the other hand, hiking GPS users might wish to have a detailed map of the terrain, rivers, hills and so forth, and perhaps tracks and trails, but not roads. They would also probably like details of things that would help them along the way and would like to make a note of all possible places to stay, and so forth. Also, they might need waypoints; locations to make for on their general route.

Finally, marine users need very specific information relating to the sea bed, navigable channels, and other pieces of maritime data. These data can help them navigate safely. All these details are needed so that the boat does not become grounded due to shallow areas or un-navigable currents.

These days GPS systems don't just tell you where you are, they also tell you where you need to go

A special kind of GPS system that is built to help fishermen is called the fishfinder. This consists of both GPS and sonar, along with some tracking functions. This can be used by fishermen to locate themselves and also to track movements of shoals of fish in real time. It can also be used to predict the movement of the fish. This also means that fishermen can now cooperate by relaying information about their locations. This can also help them to find the best waters for fishing.

Recent GPS systems also have the capability to plan and make your own routes. They do this using a variety of features.

Another important system is the Geographic Information System (GIS). GIS provides information for describing and mapping geographic features. The GPS tells us "where" while the GIS tells us "what". A complete knowledge of GPS and GIS enables us to locate, organise, analyze and map all our resources. One of these features concerns waypoints.

A waypoint is based on coordinates entered into a GPS receiver's memory. It can be either a saved position fix, or user entered coordinates. It can be created for any point on the planet. It must have a receiver designated code or number, or a user supplied name. Once entered and saved, a waypoint remains unchanged in the receiver's memory until edited or deleted.

Thus, there is no doubt that GPS has transformed the lives of millions of people. It is a landmark invention which ensures that, as long as you have a view of the sky above you, you will never be lost again.

Workshop: How to use a GPS receiver

Knowing how to use a GPS is as important as actually having one. If you are the type of person who is adventurous at heart but does not do many of the things that you long to because of the fear of getting lost, then a GPS would be your ideal solution. However, there are many small things to be kept in mind when you are operating a GPS receiver.

There are four basic functions provided by any GPS receiver: location, distance/direction info, route creation and tracking.

Finding a location

A GPS unit accurately triangulates your position by receiving data transmissions from multiple orbiting satellites. Your location is given in latitude and longitude.

Route navigation

A location or destination is called a "waypoint." For example, you can establish a starting waypoint at a trailhead by using the location function. All you need to do is to specify the coordinates of the place that you want to go to (which will need to be taken from Google Earth or a book or something) and a GPS can give you a straight-line, point-to-point bearing and distance to your destination. However, owing to the tendency of trails to never follow a straight path, the bearing changes as you go along. The indicated distance to travel will also decrease as you approach your goal.

Finding your way out in unfamiliar terrain is easy with a GPS receiver along

Route creation

By combining multiple waypoints on a trail, you can move point-to-point with intermediate bearing and distance guides. Once you reach the first predetermined waypoint, the GPS receiver can automatically point you to the next one or you can manually do this.

Tracking

One of the most important features of a GPS system is its ability to let you lay out a track. A track is like a path that you create which tells you how you have reached a particular place. This differs from a "route," which details where you're going. You can configure a GPS to automatically drop "trackpoints" over intervals of either time or distance. To retrace your steps, simply follow the GPS bearings back through the sequence of trackpoints.

Depending on the algorithm used by the GPS system, two receivers mounted even on the same antenna can give varied results

To provide reliable navigational information a GPS receiver needs to receive good signals from at least four satellites. In order to acquire the signals from the satellites, all that needs to be done is to turn on the GPS receiver and go to the satellite screen. This will display the current configuration of the satellites and the strength of the signals. It may take several minutes for the GPS unit to lock in to the satellites. In case there are only a few satellites present or the signals from the satellites are all weak, it is always advisable to simply use a map and a compass.

Most GPS receivers automatically select the satellites used in the timing solution. This makes them easy to use. Often, you simply turn the receiver on and wait for a signal to be acquired. However, the algorithms used by all the GPS receivers are all different. The decision to keep or to drop a particular satellite’s signal is also completely based on the algorithm. Some algorithms choose the satellites that provide the best geometric dilution of precision (GDOP). Others choose the satellites highest in the sky after a fixed position has been entered. Some algorithms limit the timing solution to just one, or just a few satellites. Others can use as many as 12 satellites in the solution. For this reason, two GPS receivers can obtain very different results even when connected to the same antenna in the same location.

The optimum satellite lock occurs when there is a clear view of the sky above. Tree canopy, canyons and tall buildings that obscure the view overhead or obscure the view of the horizon can impede reception. Thus it is best to go to a clearing or a high point where you can get a stronger signal.

Most receivers allow the use of a fixed position, after which no further positions are computed. However, some receivers cannot turn off position fixes, which makes them a poor choice for a frequency standard. Even though the receiver is stationary, it will appear to be moving, and the position errors will contribute large fluctuations to the frequency.

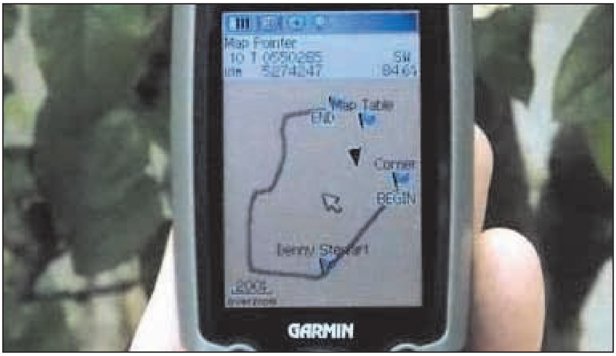
It is always best to keep the following points in mind

- A GPS unit does NOT replace a map and compass.
- A GPS unit is only as good as the map you use with it.
- For top performance, your GPS unit may need to be initialised.
- Before using your GPS receiver as a primary navigational tool in unfamiliar territory, familiarise yourself with all of the unit's features and controls. Read the owner's manual. Practice in your neighbourhood or in a local park until you're comfortable with how everything works.

Reading coordinates

To simplify map navigation, a system of coordinates is used. Coordinates divide the map into a grid and identify a particular location by listing its relative position. The standard way of specifying the coordinates is by latitude and longitude.

DMS (Degrees/Minutes/Seconds):



You can identify trail landmarks as waypoints

The compass screen offers a wealth of useful information

This feature displays your elevation and helps forecast the weather

N47°37'12" W122°19'45".

In this example, N47° 37' 12" indicates that the north/south position is 47 degrees, 37 minutes and 12 seconds north of the equator; while W122° 19' 45" places the east/west position at 122 degrees, 19 minutes and 45 seconds west of the Prime Meridian (at Greenwich, England).

8.2 Wireless power transfer

In a world where energy is of paramount importance, it is imperative that there be an extremely efficient means of power transfer. Attenuation and energy loss due to physical media is one of the most critical and thought about problems in the process of energy transfer. The efficiency of electrical energy transfer is often dependant on the length of the cable through which it is transferred and as a result, there are often massive losses in power.

For a long time, a solution to this problem has been considered to be wireless power transfer. The theory of wireless transfer of energy was first made possible by the discovery of Ampere's law and Faraday's law of induction, discovered in 1830 and 1831 respectively. The pioneer in the field of wireless power transfer is considered to be Nikola Tesla. He has many achievements to his name in this field. He carried out wireless illumination of phosphorescent bulbs of his design at the World's Columbian Exposition in Chicago. In 1894, he lit up vacuum tubes at the 35 South Fifth Avenue laboratory, and later at the 46 E. Houston Street laboratory in New York City by means of "electrodynamic induction". In 1897 he filed the first of his patent applications dealing with wireless transmission of energy and information.

Wireless energy transfer has been thought about for decades by scientists all over the world. There were many experiments done and some have been successful to some extent.

Wireless energy transfer can be divided into near field and far field energy transfer. Near field transfer involves the transfer of energy across distances comparable to, or a few times the size of the device. This can be carried out in two ways. Either it is by induction or by resonant induction.